UNIVERSIDADE FEDERAL DE SERGIPE – UFS
CENTRO DE CIÊNCIAS SOCIAIS E APLICADAS
DEPARTAMENTO DE DIREITO
TRABALHO DE CONCLUSÃO DE CURSO

JULIA PRADO DANTAS

TENSÃO ENTRE O DIREITO À PRIVACIDADE E O DIREITO À INFORMAÇÃO DIANTE DAS NOVAS TECNOLOGIAS

SÃO CRISTÓVÃO/SE
2020

JULIA PRADO DANTAS

TENSÃO ENTRE O DIREITO À PRIVACIDADE E O DIREITO À INFORMAÇÃO DIANTE DAS NOVAS TECNOLOGIAS

Trabalho de Conclusão de curso apresentado ao Departamento de Direito da Universidade Federal de Sergipe, como pré-requisito para obtenção do título de Bacharel em Direito.

Orientação: Prof. Dr. Lucas Gonçalves Da Silva

SÃO CRISTÓVÃO/SE

2020

JULIA PRADO DANTAS

TENSÃO ENTRE O DIREITO À PRIVACIDADE E O DIREITO À INFORMAÇÃO DIANTE DAS NOVAS TECNOLOGIAS

Trabalho de Conclusão de curso apresentado ao Departamento de Direito da Universidade Federal de Sergipe, como pré-requisito para obtenção do título de Bacharel em Direito.

São Cristóvão-SE, XX de setembro de 2020

BANCA EXAMINADORA

_____

Professor Doutor Lucas Gonçalves da Silva

_____

BANCA EXAMINADORA

_____

BANCA EXAMINADORA

AGRADECIMENTOS

Quando iniciei essa jornada cinco anos atrás, não imaginava quantas pessoas incríveis estariam ao meu lado, torcendo por mim e pegando as pedras no meio do caminho para que eu pudesse construir o meu castelo.

Aos meus pais, que me banham com seu amor sem limites e me apoiaram do início ao fim. Pai, Mãe, obrigada por todos os ensinamentos ao longo dos anos, principalmente o valor da educação, cujos benefícios colherei por toda a vida. A Flavia, minha irmã, que sempre me inspira com suas palavras a dar o meu melhor. Agradeço também a toda a minha família, que zela pelo meu bem-estar e sucesso mesmo à distância.

Também sou muito grata às amizades que fiz na UFS, especialmente Emily, Fabi e Flavinha, que me acompanharam desde o primeiro período e estão ao meu lado desde então. Minha graduação não seria a mesma sem vocês para a iluminarem, meu afeto é incondicional. A minha amiga de longa data, Fabi, que sabe o valor que dou a esta conquista.

Quero agradecer especialmente ao pessoal do RPG, Balão, Fela, Gus, Lua e Mika, que semanalmente me faziam sair da minha cabeça para ser parte de um novo mundo.

Agradeço ao meu orientador, o professor Dr. Lucas Gonçalves da Silva, por ter aceitado participar dessa jornada de desbravamento em um tema ainda tão pouco explorado pelo Direito.

Mesmo palavras não bastando para expressar minha felicidade, gostaria de agradecer a todos vocês, que acreditam em meus sonhos e na minha capacidade para alcançá-los.

"*O fim do Direito não é abolir nem restringir, mas preservar e ampliar a liberdade*"

John Locke

RESUMO

A revolução tecnológica ocorrida ao longo dos últimos anos promoveu uma verdadeira evolução na comunicação, permitindo que as informações sejam transmitidas de forma fácil e rápida. O Direito enfrenta diversos dilemas enquanto adapta-se à realidade digital, que carece de regulamentação. Em face desse contexto, o presente trabalho tem como objetivo realizar, através de uma revisão bibliográfica da doutrina, jurisprudências e das leis atualmente em vigor no Brasil, uma análise acerca da proteção do direito à privacidade e sua colisão com o direito à informação na modernidade, assim como as transformações pelas quais passaram desde sua origem, principalmente aquelas decorrentes do desenvolvimento tecnológico recente. Em um segundo momento, observa-se como os legisladores e tribunais lidam com essas mudanças, além das dificuldades em regular a internet, culminando no exame do panorama mundial da proteção de dados, especialmente no Brasil, com destaque para a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e os princípios que a regem. Ao final do trabalho, verifica-se que normas criadas especificamente para a proteção da privacidade na sociedade da informação são um bom primeiro passo, mas estas só serão eficazes se conseguirem manter-se atuais frente ao constante desenvolvimento tecnológico.

Palavras-chave: Direito à privacidade; Direito à informação; Lei nº 13.709/2018; Sociedade da Informação

ABSTRACT

The technological revolution that happened in the last few years has promoted a true evolution in the realm of communication, allowing information to be transmitted in an easy and fast way. Law faces many challenges while it adapts to the digital reality, that lacks regulation. In this context, the current work aims to perform, through a bibliographical review of the legal literature and laws currently in force in Brazil, an analysis on the right to privacy and its friction with the right to information in the modern age, along with the transformations these have been through since their origins, mainly those arising from recent technological developments. In a second moment, it is observed how the legislators and courts deal with these changes, as well as the difficulties of regulating the internet, culminating in the examination of the worldwide perspective on data protection, especially in Brazil, highlighting the General Protection Law of Personal Data (Law n. 13.709/2018) and the principles that conduct it. At the end of this work, it is verified that the laws created specifically for privacy protection in the information society are an adequate first step, but these will only be effective if they manage to maintain updated in the face of the constant technological development.

Keywords: Right to privacy; Right to information; Brazilian Law nº 13.709/2018; Information society

SUMÁRIO

INTRODUÇÃO

O direito à privacidade é uma garantia antiga e bastante ampla que ganha novos contornos em decorrência do avanço tecnológico nos dias atuais, expandindo os ambientes de comunicação. Desde o início da revolução tecnológica, existem debates no mundo jurídico acerca de como enfrentar os desafios trazidos por esta, já que os meios existentes não bastam para tal.

O objetivo deste trabalho é analisar o direito à privacidade e o direito à informação, seu desenvolvimento ao longo do tempo e como eles se apresentam na era tecnológica. Tal estudo servirá como base para explorar a aplicação do ordenamento jurídico no ambiente virtual, tanto enquanto adaptação como na forma de inovação.

No primeiro capítulo, através de uma perspectiva histórica, observa-se a origem do direito à privacidade e seu fortalecimento como garantia, em parte graças ao reconhecimento dado por diversos documentos internacionais. São exploradas então as várias dificuldades enfrentadas por aqueles que tentam defini-la, chegando-se a um conceito aproximado desse direito.

Em seguida, são analisadas algumas das medidas de proteção à privacidade adotadas no Brasil, inclusive na forma de normas que não traziam tal objetivo como principal.

Ainda no primeiro tópico, há um breve estudo do direito ao esquecimento, fundamentado na privacidade e objeto de algumas decisões judiciais, cujo conteúdo será devidamente abordado com a finalidade de demonstrar quais são os argumentos utilizados em sua defesa.

Encerrando essa seção, é apresentada a influência exercida pela sociedade da informação no direito à privacidade, que aprofunda-se e é submetido a novas ameaças, especialmente como consequência da expansão tecnológica, tendo como resultado a alteração de seu conceito.

Por sua vez, o segundo capítulo aborda uma garantia que muitas vezes entra em conflito com a privacidade: O direito à informação e ao seu acesso. Funciona, assim, como lembrete constante de que a intimidade não é absoluta, e nem deve ser.

Inicialmente, esse tópico assemelha-se ao anterior, trazendo um breve histórico da informação, com destaque para as mudanças ocasionadas pelo desenvolvimento de diferentes meios de comunicação. Também explora o processo de consolidação do acesso à informação enquanto direito, de seu surgimento como tal até os dias atuais.

Prossegue então para a previsão do acesso à informação no Brasil, colocando em evidência as disposições normativas mais recentes, especialmente a Lei 12.527/2011 (Lei de Acesso à Informação), que busca não apenas garantir esse direito, como também concretizá-lo.

Enfim, o segundo tópico encerra-se com a análise de como as novas tecnologias – especialmente a internet – transformaram os meios de comunicação, levando à renovação do direito à informação e do próprio modo como seu acesso é efetivado.

O terceiro capítulo traz uma face mais sombria da sociedade da informação, examinando como a constante exposição pode levar a um Estado de vigilância e segurança, onde os indivíduos têm sua esfera privada constantemente violada sob o argumento de proteção da segurança coletiva.

Também investiga-se quais efeitos a transparência tem na sociedade e nos indivíduos em geral, assim como que fatores são responsáveis pela manutenção desse sistema, questionando-se sua validade.

No quarto tópico, apresenta-se a influência que as novas tecnologias têm no direito como um todo, as alterações trazidas por elas e as adversidades decorrentes tanto para aqueles que criam as normas quanto para quem as aplica. Além disso, aborda a necessidade de enfrentar tais desafios, mesmo que de forma imperfeita.

Primeiramente, é explorado o direito de acesso à informação – considerando-se também a ampliação do próprio conceito de “informação” – e quais são as modificações necessárias para promover a sua concretização e preservação no meio ambiente digital.

Retoma-se então a análise do direito à privacidade e do direito ao esquecimento, ambos em confronto constante com diversos aspectos da sociedade da informação. Ao mesmo tempo, é graças a essa aparente incompatibilidade que tais garantias encontram-se em evidência atualmente.

No caso de ambos os direitos fundamentais, decisões de tribunais servem de suporte para um melhor entendimento de como o atrito entre eles tem sido resolvido até então e pode ser abordado no futuro.

Por fim, o tópico cinco dedica-se ao panorama da proteção de dados pessoais no mundo, especialmente as Diretivas do Parlamento Europeu e do Conselho da Europa. A seguir, direciona-se ao estudo da legislação nacional, em específico a Lei Geral de Proteção de Dados Pessoas (Lei nº 13.709/2018) e dos princípios que regulam o tratamento de tais informações no Brasil.

1 – DIREITO À PRIVACIDADE

1.1. ORIGEM E CONCEITO

A privacidade em si – não como direito – é um conceito recente, originário da Revolução Industrial e das transformações socioeconômicas por ela desencadeadas, como a separação entre o local de trabalho e a morada. Ainda naquela época, ela era limitada àqueles que dispunham dos recursos para realizá-la, ou seja, a classe burguesa.

> [...] o nascimento da privacidade pode ser historicamente associado à desagregação da sociedade feudal, na qual os indivíduos eram todos ligados por uma complexa série de relações que se refletiam na própria organização da vida cotidiana: o isolamento era privilégio de pouquíssimos eleitos ou daqueles que, por necessidade ou opção, viviam distantes da comunidade (RODOTÁ, 2008, p. 26)

Consagrada desde o Século XVI nos ordenamentos jurídicos estrangeiros, a privacidade foi reconhecida pela primeira vez como direito em 1890, no artigo “The Right to Privacy”[1]. De autoria de Samuel Warren e Louis Brandeis, definiu-se inicialmente que a privacidade seria o direito de estar só.

Como direito da personalidade, o fortalecimento da privacidade acompanha o reconhecimento ou consolidação de outros direitos da personalidade, como o direito a publicidade e o direito à identidade pessoal, ambos relacionados ao modo de apresentação do indivíduo diante da sociedade.

O direito à privacidade é garantia essencial ao pleno desenvolvimento do cidadão e ao exercício pleno da liberdade de pensamento, crença e consciência, estas últimas garantidas na Declaração Universal dos Direitos Humanos de 1948.

> Artigo XVIII – Todo ser humano tem direito à liberdade de pensamento, consciência e religião; este direito inclui a liberdade de mudar de religião ou crença e a liberdade de manifestar essa religião ou crença, pelo ensino, pela prática, pelo culto e pela observância, em público ou em particular. (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2009, p. 10)

---

1 Vânia Siciliano Aieta (1999, p. 80-82) explica que a despeito da existência de alguns antecedentes europeus, a publicação do famoso ensaio “The Right to Privacy” significou um divisor de águas no tocante à consagração do direito à intimidade. Com o ensaio, a matéria passou a ser tratada com o status de teoria, propiciando as bases técnico-juridicas da noção de privacy e configurando-a como um real “right to be let alone”

Além disso, o direito à privacidade é reconhecido como direito próprio na Declaração Universal (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2009, p. 8), onde está determinado que “ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação”.

Como parte do rol de direitos humanos, é um direito inato e inerente, pertencendo a todas as pessoas, independentemente do cumprimento de qualquer condição. Bem como é intransmissível, imprescritível e impenhorável, e todas essas características somente ressaltam a sua importância.

Destaque-se também que a privacidade é um direito fundamental tanto de dimensão objetiva quanto de dimensão subjetiva. Neste último, define-se como a possibilidade que todos possuem de impedir a invasão de outrem em sua vida privada, controlando os próprios dados pessoais. Já em seu caráter objetivo, representa a essência da democracia, proporcionando o exercício das liberdades anteriormente citadas.

Para Celso Bastos e Ives Martins (1989, v.2, p. 63), a privacidade pode ser definida como

> […] faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área da manifestação essencial do ser humano.

Além dele, muitos outros estudiosos tentaram definir o direito à privacidade. Para Westin, é “controlar a maneira na qual os outros utilizam as informações a nosso respeito”, enquanto Friedman vai além ao determinar que é “a proteção de escolhas de vida contra qualquer forma de controle público e estigma social”, ambos trazidos por Stefano Rodotá (2008. p. 15).

A partir desses conceitos é possível concluir que a intimidade deriva do direito de liberdade, é fundamental para este que o indivíduo seja capaz de resguardar sua individualidade e realizar condutas sem que seja exposto ao Estado ou à sociedade que integra. É nessa esfera pessoal protegida pelo direito à intimidade que o sujeito pode desenvolver a sua personalidade e evoluir como ser humano aquém às interferências externas.

> Neste diapasão, permitir que o indivíduo exponha suas opiniões é considerado primado básico do estado democrático de direito, e não se questiona seu valor. Esta liberdade é fundamental no desenvolvimento da personalidade, servindo também de fundamento para o exercício de outras liberdades (BARROSO, 2007, p. 63-100)

O caso Griswold v. Connecticut, ocorrido em 1965, é um bom exemplo de como se daria tal proteção. Nele, a Suprema Corte dos Estados Unidos da América reconheceu a existência do direito à intimidade, mesmo ele não estando enumerado em sua Constituição[2], considerando inconstitucional lei estadual que vedava o uso de meios anticoncepcionais. Esse e outros casos similares enxergam o direito à privacidade como uma proteção contra a intromissão governamental.

Para melhor entender a privacidade, pode-se recorrer à teoria das esferas de Hubmann e Henkel, citada por Maurício Leonardi (2011, p. 58). Ela considera que a privacidade está contida em três esferas, cada qual representando uma nova camada de informação. Na mais externa está contido tudo aquilo que está à disposição daqueles que se interessarem, intermediariamente encontra-se o que poderia ser compartilhado com o círculo íntimo do sujeito, como sua família e amigos próximos, por fim, no núcleo estão contidas a intimidade e segredos do indivíduo.

Apesar de ser uma forma interessante de analisar a privacidade, não deixa de ser incompleta, conforme dispõe Leonardi (2011, p. 60):

> Ocorre, porém, que não há uma relação necessária entre o “grau de intimidade” de determinada informação e os danos causados por sua divulgação. Por meio da agregação de dados isolados e fragmentos de informação aparentemente irrelevantes, é possível montar perfis completos a respeito de um indivíduo, revelando inúmeros aspectos de sua personalidade, sem que se tenham coletado quaisquer informações íntimas de seu exclusivo conhecimento.

No entanto, frise-se que tal indeterminação do conceito de intimidade é fundamental para a sua própria proteção, já que possibilita a sua mutabilidade, adaptando-se a diferentes circunstâncias históricas e sociais. Embora possua variações de intensidade e conteúdo, a privacidade possui relevância em todas as culturas, locais e épocas.

---

2 Os Juízes William O. Douglas, Arthur Goldberg, Byron White e John Marshall Harlan II defenderam que o direito à privacidade emanava de outras proteções constitucionais, como o devido processo legal e a vedação à autoincriminação.

Na sociedade moderna, a proteção à vida privada dos indivíduos é um direito fundamental relacionado à dignidade da pessoa humana. Como direito fundamental, é um elemento essencial da Constituição de qualquer Estado constitucional, inclusive do Brasil.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> […]
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

O ordenamento jurídico brasileiro traz tanto o direito do titular de exigir a abstenção do Estado e de terceiros em sua intimidade e vida privada quanto a sua faculdade de exigir do poder público a efetividade da norma, vedando a omissão estatal frente a ameaças de terceiros. Ambos os aspectos são fundamentais para a eficácia plena do direito à privacidade.

Apesar de muitas vezes serem usados como sinônimos, há certa distinção entre a intimidade e a vida privada, dois atributos do direito em discussão que diferenciam-se principalmente pela menor amplitude do primeiro. Em Sidney Guerra (2004, p. 55), há alguns apontamentos relevantes acerca dessa relação, contribuindo para a diferenciação entre os termos:

> Assim, para melhor esclarecimento, verifica-se que a intimidade é algo a mais do que a vida privada, ou seja, a intimidade caracteriza-se por aquele espaço, considerado pela pessoa como impenetrável, intransponível, indevassável e que, portanto, diz respeito única e exclusivamente a pessoa, como, por exemplo, recordações pessoais, memórias, diários, etc. Este espaço seria de tamanha importância que a pessoa não desejaria compartilhar com ninguém. São os segredos, as particularidades, as expectativas, enfim, seria, o que vamos chamar de ‘o canto sagrado’ que cada pessoa possui. Já a vida privada consiste naquelas particularidades que dizem respeito, por exemplo, à família, problemas envolvendo parentes próximos, saúde física e mental etc. Seria então aquela esfera íntima de cada um, que vedasse a intromissão alheia. Entretanto, percebe-se que neste caso a pessoa poderia partilhá-la com as pessoas que bem lhe conviesse, sendo da família ou apenas um amigo próximo.

Ainda é possível complementar tal definição com os ensinamentos trazidos por Gilmar Ferreira Mendes e Paulo Gustavo Gonet Branco (2015, p. 282), que preceituam que “no âmago do direito à privacidade está o controle de informações

sobre si mesmo", englobando não apenas as informações relacionadas a intimidade, mas também aquelas ligadas a dados pessoais que podem levar à identificação de seu titular.

Tal direito à privacidade informacional ou direito à autodeterminação informativa tem recebido cada vez mais destaque frente a ascensão da tecnologia, devendo ser considerado o seu alcance tendo-a em mente. Para Rodotá (2008, p. 139), "nascida como exigência essencialmente individual, a privacidade requer cada vez mais uma construção social", e é isso que será tratado a seguir.

1.2. DIREITO À PRIVACIDADE NO BRASIL

A história da proteção ao direito à privacidade no Brasil é bastante recente, iniciando-se de forma tímida na legislação infraconstitucional nos anos após a promulgação da Constituição Federal de 1988.

Na Lei nº 8.159/1991, estava disposto que os documentos "necessários ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas são originariamente sigilosos" (Art. 23, §1º), exigindo, portanto, fundamentação para a sua divulgação.

No mesmo sentido dispõe o Pacto de San José da Costa Rica, recepcionado por meio do Decreto 678 de 1992, onde veda-se a interferência excessiva na vida privada dos indivíduos, visto que seu artigo 11 determina que "ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada".

Destaque-se que o direito à privacidade e ao sigilo também foi garantido em relação aos documentos públicos, conforme disposição da já revogada Lei nº 11.111/2005:

> Art. 7º Os documentos públicos que contenham informações relacionadas à intimidade, vida privada, honra e imagem de pessoas, e que sejam ou venham a ser de livre acesso poderão ser franqueados por meio de certidão ou cópia do documento, que expurgue ou oculte a parte sobre a qual recai o disposto no inciso X do caput do art. 5º da Constituição Federal.

Apesar da consagração do direito à privacidade ser tomada no sentido amplo, possibilitando assim a inclusão de todas as suas manifestações, deve-se lembrar que não existe direito absoluto, podendo a privacidade ser mitigada em face de

circunstâncias concretas, sendo esse o entendimento tanto da doutrina quanto do Supremo Tribunal Federal.

> EMENTA: PROCESSO PENAL. PRISÃO CAUTELAR. EXCESSO DE PRAZO. CRITÉRIO DA RAZOABILIDADE. INÉPCIA DA DENÚNCIA. AUSÊNCIA DE JUSTA CAUSA. INOCORRÊNCIA. INDIVIDUALIZAÇÃO DE CONDUTA. VALORAÇÃO DE PROVA. IMPOSSIBILIDADE EM HABEAS CORPUS […] Na contemporaneidade, não se reconhece a presença de direitos absolutos, mesmo de estatura de direitos fundamentais previstos no art. 5º, da Constituição Federal, e em textos de Tratados e Convenções Internacionais em matéria de direitos humanos. Os critérios e métodos de razoabilidade e da proporcionalidade se afiguram fundamentais nesse contexto, de modo a não permitir que haja prevalência de determinado direito ou interesse sobre outro de igual ou maior estatura jurídico-valorativa. (STF – HC: 93250 MS, Relator: Min. Ellen Gracie, Data de Julgamento: 10/06/2008, Segunda Turma, Data de Publicação: DJe-117 DIVULG 26-06-2008 PUBLIC 27-06-2008 EMENT VOL-02325-04 PP-00644)

Em 2011, surgiu a Lei nº 12.527, norma infraconstitucional que regula com mais detalhes a relação entre acesso à informação e direito à privacidade, além de destacar que este último se refere a todos os dados de natureza pessoal do indivíduo.

Conhecida como Lei de Acesso à Informação, essa norma tem como destinatário específico o Estado, englobando seus órgãos públicos e entidades, o que não impede que suas disposições sirvam de inspiração para o tratamento de dados em outros âmbitos.

> Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
>
> § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
>
> I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem;
> […]

Apesar de reconhecer que a privacidade referente às informações pessoais merece tratamento especial, a norma só menciona a responsabilidade de órgãos e entidades públicas ou daqueles que possuam vínculo com estas, negligenciando grande parte dos “vazamentos” de informações.

Isso se deve ao fato de que a Lei de Acesso à Informação serve como guia especialmente para a administração pública, como será explorado mais a frente, e, portanto, não abrange muitas das situações de violação desse direito, especialmente na modernidade.

Ademais, embora seja dado merecido enfoque ao direito à reparação, são deixadas de lado punições referentes ao compartilhamento de informações se este não causar dano ao indivíduo. Essa é uma consequência do tratamento dado à privacidade pela própria Constituição, que enuncia no art. 5º, X, que é “assegurado o direito a indenização pelo dano material ou moral” em casos de violação desse direito.

> Art. 34. Os órgãos e entidades públicas respondem diretamente pelos danos causados em decorrência da divulgação não autorizada ou utilização indevida de informações sigilosas ou informações pessoais, cabendo a apuração de responsabilidade funcional nos casos de dolo ou culpa, assegurado o respectivo direito de regresso.
>
> Parágrafo único. O disposto neste artigo aplica-se à pessoa física ou entidade privada que, em virtude de vínculo de qualquer natureza com órgãos ou entidades, tenha acesso a informação sigilosa ou pessoal e a submeta a tratamento indevido.

A própria jurisprudência dos tribunais superiores deixa a desejar em termos de medidas punitivas que sejam distintas da indenização, as quais somente recebem destaque em situações que envolvem o direito ao esquecimento.

1.3. DIREITO AO ESQUECIMENTO

Fundamentado no direito à privacidade, à intimidade e à honra (assegurados no art. 5º, X, da CRFB/88), o direito ao esquecimento é o direito que uma pessoa possui de não permitir que um fato, mesmo que verídico, ocorrido em certo momento de sua vida, seja continuamente exposto ao olhar público, causando-lhe sofrimento ou transtornos. Nas palavras de François Ost (2005, p. 160):

> Uma vez que, personagem pública ou não, fomos lançados diante da cena e colocados sob os projetores da atualidade – muitas vezes, é preciso dizer, uma atualidade penal –, temos o direito, depois de determinado tempo, de sermos deixados em paz e a recair no esquecimento e no anonimato, do qual jamais queríamos ter saído.

No mesmo sentido discorre o Ministro Gilmar Ferreira Mendes, junto a Paulo Branco (2015, p. 286) ao dispor que “Se a pessoa deixou de atrair notoriedade, desaparecendo o interesse público em torno dela, merece ser deixada de lado, como desejar”, retomando a noção da privacidade como o “direito de estar só”.

O caso mais citado acerca desse direito é o Lebach (ALEXY, 2008, p. 100), julgado pela Suprema Corte alemã. Uma emissora tinha a intenção de exibir documentário que contava a história do assassinato de quatro guardas alemães em incidente ocorrido em 1969. Um dos condenados pelo crime estava prestes a ser solto, por cumprimento da pena, às vésperas da veiculação do programa, que apresentava fotos reais e nomes de todos os envolvidos.

Na discussão processual que se seguiu, argumentou-se que não havia mais um interesse atual pela notícia do crime, além do possível prejuízo à ressocialização do condenado. Com base nisso, o Tribunal Constitucional alemão decidiu que deveria prevalecer o direito do condenado frente a liberdade de informação da emissora (ALEXY, 2008, p. 101-102).

Conclui-se assim que, desde sua origem, o direito ao esquecimento está intimamente relacionado ao “controle de informações sobre si mesmo” (MENDES; BRANCO, 2015, p. 282), parte central da privacidade. Além disso, não se pode esquecer de sua importante relação com o princípio fundamental da dignidade da pessoa humana, sendo esse inclusive o conteúdo do Enunciado 531 da VI Jornada de Direito Civil do CJF/STJ[3].

No entanto, apesar de ser objeto de discussão já a muitos anos na Europa e nos Estados Unidos, a questão ainda é pouco debatida nos tribunais brasileiros, que costumam dar mais atenção a outras dimensões do direito à privacidade. A prova disso é que somente em 2013 o Superior Tribunal de Justiça se manifestou no mesmo sentido que a Suprema Corte alemã, garantindo o direito ao esquecimento no julgamento do REsp 1.334.097-RJ[4].

---

3 Enunciado 531: A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento.

4 Situação da “Chacina da Candelária”: Determinado indivíduo foi acusado de ter participado da Chacina, sendo, no entanto, posteriormente absolvido. Anos após o fato, a rede Globo, no programa “Linha Direta” apontou o nome desse homem como um dos envolvidos no crime e que foi absolvido. No caso concreto, o STJ entendeu que o réu condenado ou absolvido pela prática de crime tem garantido o direito ao esquecimento, associando-o ao sigilo da folha de antecedentes e a exclusão dos registros da condenação no instituto de identificação, direitos garantidos pelo art. 748 do CPP.

François Ost (2005, p. 161) traz interessante decisão do Tribunal de última instância de Paris (Mme. Filipachi Cogedipresse, de 20 de abril de 1983), onde este direito foi assegurado, reafirmando assim a sua importância para a sociedade como um todo.

> (...) qualquer pessoa que se tenha envolvido em acontecimentos públicos pode, com o passar do tempo, reivindicar o direito ao esquecimento; a lembrança destes acontecimentos e do papel que ela possa ter desempenhado é ilegítima se não for fundada nas necessidades da história ou se for de natureza a ferir sua sensibilidade; visto que o direito ao esquecimento, que se impõe a todos, inclusive aos jornalistas, deve igualmente beneficiar a todos, inclusive aos condenados que pagaram sua dívida para com a sociedade e tentam reinserir-se nela.

Entretanto, não se deve esquecer importante exceção, ressaltada pelo Ministro Luís Felipe Salomão no julgamento do REsp 1.335.153-RJ[5]: "ressalvam-se do direito ao esquecimento os fatos genuinamente históricos – historicidade essa que deve ser analisada em concreto – cujo interesse público e social deve sobreviver à passagem do tempo".

Ou seja, ao sopesar ambos os direitos constitucionalmente tutelados, o juízo deve considerar que a inserção em fato de interesse coletivo mitiga a proteção à intimidade e à privacidade em prol do interesse público.

Conclui-se assim que o grande desafio relativo ao chamado direito ao esquecimento diz respeito à amplitude de sua incidência, devendo ser ponderado com outras garantias constitucionais, como o direito à informação, à memória[6] e à liberdade de expressão.

Além disso, com o advento da internet, onde os dados ficam armazenados em diversos servidores ao redor do mundo, surgem novos desafios à garantia do direito ao esquecimento, que serão analisados em tópico próprio.

---

5 Caso "Aida Curi": Os familiares de Aida Curi, abusada sexualmente e morta em 1958 no Rio de Janeiro, moveram ação contra a Rede Globo que, também no programa "Linha Direta", divulgou o nome da vítima e fotos reais do crime. Nesse caso, a 4ª Turma do STJ entendeu que o crime em questão foi um fato histórico, de interesse público e que seria impossível relatá-lo sem a menção ao nome da vítima. Na ementa, constou: "(...) o direito ao esquecimento que ora se reconhece para todos, ofensor e ofendidos, não alcança o caso dos autos, em que se reviveu, décadas depois do crime, acontecimento que entrou para o domínio público, de modo que se tornaria impraticável a atividade da imprensa para o desiderato de retratar o caso Aída Curi, sem Aída Curi."

6 O direito à memória foi regulamentado pela Lei nº 12.528/2011, que criou a Comissão Nacional da Verdade, destinada a apurar as circunstâncias em que ocorreram violações a direitos humanos durante o período de ditadura militar.

1.4. PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO

O conceito de privacidade esteve em constante mutação ao longo dos anos, sendo profundamente afetado pela revolução digital e pela globalização, que relativizam a própria noção de inviolabilidade da intimidade. Consequentemente, a sua definição deve ser modificada para garantir uma maior proteção a esse direito fundamental na sociedade da informação.

Para Silva (2013, p. 132), o direito à intimidade é o direito de "defender e preservar um âmbito íntimo, variável segundo o momento histórico imperante, no qual estas possam desenvolver sua personalidade, bem como o poder de controlar suas informações pessoais". Na sociedade da informação,

> Estamos diante da possibilidade de um controle social cada vez mais amplo e difuso, exercido pelos centros de poder públicos e privados. Este controle, em relação aos indivíduos, pode assentar obstáculos reais ao livre desenvolvimento da personalidade individual, imobilizado em torno de perfis historicamente determinados.(RODOTÁ, 2008, p. 83)

Dessa forma, a privacidade adquire maior profundidade e também um novo conteúdo onde busca, levando em consideração a cultura da transparência dominante, também "resguardar o cidadão com relação aos dados informatizados" (LIMBERG, 2007, p. 58).

Com a sociedade da informação, surgem novos meios de invasão da privacidade, especialmente como consequência dos dados pessoais dos indivíduos estarem contidos em uma multitude de servidores espalhados pelo mundo. Por esse mesmo motivo, também é mais difícil identificar e punir os autores de tal violação.

> A invocação em defesa da privacidade, de fato, não parte somente de quem pretende uma garantia total de intimidade, que chegue às raias do anonimato. Com intensidade comparável, a mesma invocação é feita pelos que têm a sua privacidade violada em virtude de comportamentos de quem, permanecendo anônimo, torna impossível, ou especialmente difícil, a adoção de contramedidas. (RODOTÁ, 2008, p. 122)

De acordo com o pensamento de Rodotá (2008, p. 24), a definição de privacidade afasta-se cada vez mais da noção de "direito de ser deixado só" trazida por Samuel Warren e Louis Brandeis e aproxima-se da possibilidade de indivíduos e

grupos de pessoas poderem controlar o fluxo e disponibilização de informações. Ou seja, o direito à privacidade manifesta-se também como direito de excluir de sua esfera privada uma determinada categoria de informações.

Na sociedade da informação, as conexões são, ao mesmo tempo, públicas e privadas. Privadas pois a comunicação se dá entre indivíduos que, na teoria, possuem alguma relação de sociabilidade no mundo *offline*, mas também públicas "porque os dados e informações lá constantes, em tese, poderiam ser acessados por qualquer outro indivíduo que venha a acessar o sistema" (SILVA, 2013, p. 123).

Nesse contexto, Limberg (2007, p. 231) traz uma importante distinção acerca da intimidade na era digital:

> O direito à intimidade pode ser visto a partir de dois aspectos: a) intimidade enquanto aspecto negativo, pois se trata de um "resguardo dos dados em geral e dos dados sensíveis em particular em face das novas tecnologias" b) intimidade enquanto aspecto positivo, pois consiste no direito do indivíduo de exigir informação, o acesso, a retificação e o cancelamento de dados pessoais.

Sendo assim, a privacidade projeta-se para além de sua definição tradicional e passa a ser apresentada como parte indispensável da liberdade existencial, uma "tutela das escolhas de vida contra toda forma de controle público e estigmatização social" (RODOTÁ, 2008, p. 144).

Em 2005, alunos do Centro Haifa de Direito e Tecnologia concluíram que a definição de "direito à privacidade" - especialmente considerando a era digital – deveria ser a mais flexível e abstrata possível, possibilitando sua adaptação a uma realidade em constante mutação, chegando assim ao seguinte conceito (YAEL ONN, 2005, p. 12):

> O direito à privacidade é o nosso direito de manter um domínio sobre tudo em nossa volta, o que inclui todas aquelas coisas que fazem parte de nós, como nosso corpo, casa, pensamentos, sentimentos, segredos e identidade. O direito à privacidade nos dá a capacidade de escolher quais partes desse domínio podem ser acessada por outras pessoas, e para controlar a extensão, forma e momento do uso dessas informações que escolhemos divulgar.[7]

7 Tradução livre de "The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, thoughts, feelings, secrets and identity. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner and timing of the use of those parts we choose to disclose"

Apesar da construção de bancos de dados não ser um fenômeno contemporâneo, a sociedade de informação traz novos problemas no que se refere à sua proteção. Conforme lição de Marcel Leonardi (2011, p. 130), a Internet integra o cotidiano das pessoas em uma clara sobreposição entre *online* e *offline*, o que torna quase impossível manter o controle sobre esses dados após a sua disponibilização na rede. Sobre as consequências desse descontrole, Manuel Castells (1999, p. 90-91) já havia alertado:

> […] os cientistas da computação preveem a possibilidade de ambientes de processamento nos quais bilhões de microscópicos aparelhos de processamento de dados se espalharão por toda parte 'como os pigmentos da tinta de paredes'. Se isso acontecer mesmo, então as redes de computadores serão, materialmente falando, a trama da nossa vida.

Com a confirmação dessa previsão, da ampliação do ciberespaço, observam-se mais transformações na intimidade, levando ao nascimento do homem flexível, transparente, controlado. A privacidade é cada vez mais necessária, mas também torna-se, na mesma medida, mais frágil devido a exposição a ameaças decorrentes da tecnologia, como o vazamento de dados.

Segundo o ensinamento de Stefano Rodotá (2008, p. 129):

> [A tecnologia] altera assim, profundamente, a função sociopolítica da privacidade, que se projeta bem além da esfera privada, para se tornar elemento constitutivo da cidadania. E a sua definição, por muito tempo ligada unicamente ao 'direito de ser deixado só', dilata-se e volta-se para a direção da ideia de uma tutela global das escolhas da vida contra qualquer forma de controle público e de estigmatização social, em um quadro caracterizado pela liberdade das escolhas existenciais e políticas.

Portanto, para o fortalecimento contínuo da proteção jurídica e para a ampliação das fronteiras do direito à privacidade, é necessário considerar-se as transformações trazidas pela tecnologia e como ela afeta as estruturas de poder presentes na sociedade.

2 – DIREITO DE ACESSO À INFORMAÇÃO

2.1. HISTÓRICO ACERCA DO DIREITO DE ACESSO À INFORMAÇÃO

Desde os primórdios da humanidade, a informação tem um papel relevante nas relações interpessoais e de poder que permeiam a sociedade. Em uma época primitiva, onde utilizavam-se símbolos, e depois com o surgimento da fala e da linguagem, a troca de informações era mínima e o alcance dessa comunicação era bastante limitado.

Mesmo então, “saber é poder”[8], e a maioria dos Estados soberanos retinham a informação não apenas de outros Estados, mas também de sua própria população. Foi na Grécia antiga, explica Duchein (1983, p. 2), que o Direito à informação floresceu em sua forma mais básica através dos pedidos da população para que tivessem acesso a arquivos estatais.

Com o surgimento da Imprensa de Gutenberg por volta de 1430, o acesso à informação expandiu-se novamente, impulsionando a transmissão de dados. A partir dela o alcance das informações públicas foi ampliado, trazendo a necessidade de clareza em sua divulgação.

Na Suécia de 1776, surgiu a primeira lei que tratou de forma direta do direito de acesso à informação. Além de estabelecer a liberdade de imprensa, essa norma garantiu a todo indivíduo acesso completo e gratuito aos documentos e atos governamentais enquanto simultaneamente protegia a identidade de quem procura informação.

Apesar dessa disposição normativa sueca, a maioria do mundo seguia procedimentos que condicionavam a disponibilização das informações a uma análise, e seu fornecimento ficava a critério da administração pública. Para Norberto Bobbio (2000, p. 399), o sigilo era parte da razão de Estado:

> Durante séculos, foi considerado essencial para a arte de governo o uso do segredo. Um dos capítulos que não podiam faltar nos tratados de política, num período que dura muitos séculos (de Maquiavel a Hegel) e que se costuma chamar de razão de Estado, referia-se aos modos, formas, circunstâncias, e razões do sigilo.

8 Frase atribuída ao inglês Francis Bacon

Regina Linden Ruaro e Fernando Inglez de Souza (2017, p. 210) já diziam que a posse de dados é vista como detenção de poder, tanto no âmbito interno do Estado quanto internacionalmente. Ou seja, o controle sobre a transmissão de informações demonstra a superioridade do governante perante os seus cidadãos e frente a outros Estados soberanos.

No período pós-segunda guerra, a liberdade de expressão consolida-se como direito fundamental. Dessa forma, os direitos que são consequência dessa liberdade – incluindo-se aqui o direito à informação em análise – passaram a ser alvo de maior atenção, sendo objeto de tratados com o objetivo de protegê-los. Segundo lição de Canotilho (2014, p. 28):

> A liberdade de expressão permite assegurar a continuidade do debate intelectual e do confronto de opiniões, num compromisso crítico permanente. Com essa qualidade, ela integra o sistema constitucional de direitos fundamentais, deduzindo-se do valor da dignidade da pessoa humana e dos princípios gerais de liberdade e igualdade, juntamente com a inerente exigência de proteção jurídica. A liberdade de expressão em sentido amplo é um direito multifuncional, que se desdobra num cluster de direitos comunicativos fundamentais (Kommunikationsgrudrechte) que dele decorrem naturalmente, como seja, por exemplo, a liberdade de expressão stricto sensu, de informação, de investigação acadêmica, de criação artística, de edição, de jornalismo, de imprensa, de radiodifusão, de programação, de comunicação individual, de telecomunicação e comunicação em rede.

Dessa forma, a relação entre Direito à Informação e Direitos do Homem recebeu maior destaque, o que indubitavelmente favoreceu o acesso àquela. Em 1948, o Direito à Informação é reconhecido no artigo 19 da Declaração Universal dos Direitos Humanos[9], que coloca a transmissão de informações e ideias como direito de todo ser humano.

Esse foi um passo imprescindível para que, no ano 2000, a Comissão Interamericana de Direitos Humanos – em sua Declaração de Princípios sobre Liberdade de Expressão – alçasse o Acesso à Informação ao patamar de direito fundamental de todo indivíduo.

> “Item 4 - O acesso à informação em poder do Estado é um direito fundamental do indivíduo. Os Estados estão obrigados a garantir o exercício desse direito. Este princípio só admite limitações excepcionais que devem

9 O Artigo XIX dispõe que “todo ser humano tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras” (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2009, p. 10)

> estar previamente estabelecidas em lei para o caso de existência de perigo real e iminente que ameace a segurança nacional em sociedades democráticas" (ORGANIZAÇÃO DOS ESTADOS AMERICANOS, 2000)

Consequentemente, e conforme disposto na própria Declaração, o acesso a uma informação só pode ser negado em situações raras e pontuais, sendo esse também o entendimento da Constituição Federal da República Federativa do Brasil de 1988, que dispõe, no art. 5º, inciso XXXIII, que "todos têm direito a receber dos órgãos públicos informações […], ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado".

Nessa mesma linha, percebe-se cada vez mais a importância desse direito quando se trata da fiscalização governamental e do combate à corrupção, sendo a transparência da administração pública uma das medidas em destaque na Convenção das Nações Unidas contra a corrupção de 2003[10], conforme dispositivo abaixo transcrito:

> Artigo 13
> 1. Cada Estado Parte adotará medidas adequadas, no limite de suas possibilidades e de conformidade com os princípios fundamentais de sua legislação interna, para fomentar a participação ativa de pessoas e grupos que não pertençam ao setor público, como a sociedade civil, as organizações não-governamentais e as organizações com base na comunidade, na prevenção e na luta contra a corrupção, e para sensibilizar a opinião pública a respeito à existência, às causas e à gravidade da corrupção, assim como a ameaça que esta representa.
> Essa participação deveria esforçar-se com medidas como as seguintes:
>
> a) Aumentar a transparência e promover a contribuição da cidadania aos processos de adoção de decisões;
>
> b) Garantir o acesso eficaz do público à informação; (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2003)

Na modernidade, com diversos Tratados determinando que os Governos promovam o acesso à informação e o incorporem em suas leis, há uma ampliação do controle social, especialmente no que diz respeito à administração pública.

> […] a efetividade do direito de acesso decorre da disponibilidade de um número mais amplo de informações sobre a atividade de quem coleta dados, mas também, e sobretudo, que o direito de acesso confirma sua tendência de ser um instrumento que torna a atividade de organismos públicos e privados a mais transparente possível, efetivando institucionalmente as condições para um controle social difuso. (RODOTÁ, 2008, p. 72)

10 Aprovada no Brasil por meio do Decreto Legislativo nº 348/2005.

Embora alguns Estados autoritários sigam na contramão dessa tendência, não se pode negar que o Direito de Acesso à Informação alcançou reconhecimento global como direito fundamental, sendo também um instrumento de consolidação da democracia.

2.2. DIREITO DE ACESSO À INFORMAÇÃO NO BRASIL

Originariamente previsto nos artigos 5º, XXXIII[11], 37, §3º, II[12] e 216, §2º[13], todos da Constituição Federal, o acesso à informação é garantido no Brasil pela Lei 12.527/2011, aplicável aos órgãos públicos da administração direta e indireta, demais entidades controladas pelos entes políticos, e também às entidades privadas sem fins lucrativos que recebam, para realização de ações de interesse público, recursos públicos, conforme disposição de seus artigos 1º e 2º.

Seguindo a linha indicada pela Comissão Interamericana de Direitos Humanos e pela Convenção das Nações Unidas contra a corrupção, o acesso à informação é tratado por essa norma como direito fundamental, tendo como finalidade a alteração da cultura do sigilo que ainda é predominante em muitas áreas do setor público.

> Art. 3º Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes:
>
> I - observância da publicidade como preceito geral e do sigilo como exceção;
>
> II - divulgação de informações de interesse público, independentemente de solicitações;
>
> III - utilização de meios de comunicação viabilizados pela tecnologia da informação;

11 Art. 5º. […] XXXIII – todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;

12 Art. 37. […] § 3º A lei disciplinará as formas de participação do usuário na administração pública direta e indireta, regulando especialmente: II - o acesso dos usuários a registros administrativos e a informações sobre atos de governo

13 Art. 216. […] § 2º Cabem à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem.

> IV - fomento ao desenvolvimento da cultura de transparência na administração pública;
>
> V - desenvolvimento do controle social da administração pública.

A norma dispõe que, para que esse direito seja respeitado em toda a sua amplitude, é também essencial que seja assegurada a disponibilidade, autenticidade e integridade da informação que está sendo fornecida[14], sendo esses princípios relacionados à segurança da informação[15].

Define-se a integridade como a manutenção das condições iniciais dos dados, que não podem ser alterados senão por pessoas autorizadas. Já a autenticidade representa a identificação e registro de eventuais mudanças e daquele responsável por elas. Por fim, a disponibilidade trata da possibilidade dos indivíduos conhecerem e utilizarem a informação.

Estes três elementos buscam, em conjunto, não só o direito de acesso à informação, mas também a transparência de sua gestão e veracidade dos dados obtidos.

Ademais, a Lei de Acesso à Informação também traz em seu âmbito os procedimentos que devem ser adotados para a concretização desse direito, sendo essa indicação obrigatória segundo o art. 7º[16]. Dentre os procedimentos elencados no referido diploma, destacamos:

> Lei nº 12.527/2011
> […]
>
> Art. 10. Qualquer interessado poderá apresentar pedido de acesso a informações aos órgãos e entidades referidos no art. 1º desta Lei, por qualquer meio legítimo, devendo o pedido conter a identificação do requerente e a especificação da informação requerida.
> […]
>
> Art. 11. O órgão ou entidade pública deverá autorizar ou conceder o acesso imediato à informação disponível.
> […]
>
> Art. 12. O serviço de busca e fornecimento da informação é gratuito, salvo nas hipóteses de reprodução de documentos pelo órgão ou entidade pública consultada, situação em que poderá ser cobrado exclusivamente o valor necessário ao ressarcimento do custo dos serviços e dos materiais utilizados.

14 Essa é a disposição do art. 6º, III, da Lei 12.527/2011

15 A segurança da informação minimiza as chances de roubo de dados sigilosos, sendo regida pelos fundamentos básicos da confidencialidade, integridade, disponibilidade e autenticidade.

16 Art. 7º O acesso à informação de que trata esta Lei compreende, entre outros, os direitos de obter: I - orientação sobre os procedimentos para a consecução de acesso, bem como sobre o local onde poderá ser encontrada ou obtida a informação almejada;

> […]
>
> Art. 13. Quando se tratar de acesso à informação contida em documento cuja manipulação possa prejudicar sua integridade, deverá ser oferecida a consulta de cópia, com certificação de que esta confere com o original.
> […]

Ou seja, a informação pública pertence ao cidadão, cabendo ao Estado provê-la e atender às demandas da sociedade de forma eficaz. Conclui-se, portanto, que a Lei 12.527/2011 tem como um de seus principais objetivos a superação da cultura do sigilo e sua substituição pela cultura de acesso, o que pode ser facilitado pelas inovações tecnológicas.

2.3. TRANSFORMAÇÕES NOS MEIOS INFORMACIONAIS E NOVAS TECNOLOGIAS

Como já mencionado, o surgimento da imprensa de Gutenberg influenciou grandemente no acesso à informação, sendo um fator chave na explosão do movimento Renascentista e espalhando ideias de forma nunca antes vista (WHIPPS, 2008).

No Século XX, evoluções técnicas novamente revolucionaram a transmissão de informações, que agora se dava não apenas pela escrita, mas também através do rádio e da televisão. Esses avanços e sua importância para a sociedade foram, inclusive, objeto de análise por Melvin L. De Fleur e Sandra Ball-Rokeach (1993, p. 41):

> Durante a primeira década no novo século, o cinema virou uma forma de divertimento familiar. Isto foi seguido em 1920 pela criação do rádio doméstico e, nos anos 40, pelo início da televisão doméstica. No começo da década de 50, o rádio atingira uma maturação nos lares norte-americanos, com aparelhos adicionais dispersados pelos automóveis. Houve uma penetração múltipla sob a forma de rádios para o quarto de dormir e para a cozinha, e um número crescente de aparelhos transistorizados e miniaturizados. No final dos anos 50 e início dos 60, viu-se a televisão começar a aproximar-se dessa saturação. Na década de 1970, ela estava praticamente total nos Estados Unidos e progredia em outras partes. Novos veículos foram adicionados - tv a cabo, gravadores de videocassete, e até videotexto com reciprocidade. A comunicação de massa virara um dos fatos mais significativos e inescapáveis da vida moderna.

A tecnologia assume um papel de grande relevância nas interações entre indivíduos e destes com o meio em que estão inseridos, influenciando diretamente em suas vidas pessoais. Para Manuel Castells (1999, p. 565), “[as] redes constituem a nova morfologia social de nossas sociedades e a difusão da lógica de redes modifica de forma substancial a operação e os resultados dos processos produtivos e de experiência, poder e cultura”.

Uma dessas redes é a internet, base para a estruturação da sociedade em rede que, por possuir estruturas abertas, está sempre se expandindo e sendo submetida a inovações.

> Desta forma, o avanço da informática – resultado do fenômeno da globalização -, constitui um importante passo para o rompimento de fronteiras e a comunicação instantânea em rede, tem-se que a Internet tornou possível o surgimento de comunidades virtuais que exercem importante papel nas novas formas de sociabilidade dos indivíduos. (SILVA, 2013, p. 120)

Com a comercialização da tecnologia da internet na década de 1990, surgiu uma nova forma de comunicação que se incorporou rapidamente na vida moderna, impulsionando de forma inimaginável o acesso dos cidadãos a quaisquer tipos de informações.

Para Oliveira (2004, p. 270-271), com a globalização houve a “neutralização da distância”, a comunicação instantânea assume o dever de eliminar o problema da mobilidade no mundo, já que a proximidade física não é mais requisito para a troca de dados.

Segundo o pensamento de Olsson (2007, p. 234), a globalização e a era da informação estão intrinsecamente ligados, já que são os avanços tecnológicos dos meios de transportes e comunicações que possibilitaram a presença virtual e em tempo real de fluxo para qualquer parte do planeta.

Caracterizada pela aplicabilidade de conhecimentos e informação para a geração de conhecimentos e de dispositivos de processamento e comunicação de dados, Castells (1999, p. 68-69) conceitua que uma revolução tecnológica informacional está em andamento.

Espalhando-se rapidamente por todo o mundo – atualmente mais de metade da população mundial tem acesso a Internet[17] – essa nova tecnologia criou novas

17 Segundo dados do “World Internet Usage Statistics News and World Population Stats” (Estatísticas sobre o uso de internet e população no mundo)

formas de interação, como as mensagens instantâneas e as redes sociais, caracterizadas pela sua rapidez, grande escala e interatividade. Além disso, a maioria dos meios de comunicação tradicionais enfrentam os desafios da adaptação, sendo remodelados ou redefinidos pela internet, dando origem a novos recursos e serviços.

A interrelacionalidade de mídias, denominada de cultura de convergência por Jenkins em sua obra de mesmo nome, trouxe mudanças na dinâmica social, na percepção dos indivíduos e no modo de processamento e interpretação das informações. Para Ascensão (2002), é nessa “auto-estrada da informação” que ocorre a propagação eficiente e em larga escala de grande parte dos dados disponíveis atualmente.

> A expressão sociedade da informação define uma nova forma de organização social, política e econômica que recorre ao intensivo uso da tecnologia da informação para coleta, produção, processamento, transmissão e armazenamento de informações. (VIEIRA, 2007, p. 156)

Essa nova era é alimentada pelo ativo “informação”, indispensável para a realização da maioria das atividades relevantes. Consequentemente, o uso da tecnologia da informação é recomendado e até incentivado, impactando não só a sociedade, mas também outras áreas, como a ciência, a cultura e a política.

> O acesso, dessa forma, supera o âmbito das informações pessoais e a sua disciplina tende a se conjugar com a outra, mais geral, de um “direito à informação”, também esse encarado em uma versão ativa e dinâmica: não mais, portanto, como simples “direito a ser informado”, mas como o direito a ter acesso direto a determinadas categorias de informações, e mãos públicas e privadas. Aqui desponta claramente a ligação entre os desenvolvimentos institucionais e as inovações tecnológicas: justamente estes tornam possível propor uma generalização do direito de acesso, no momento em que eliminam os obstáculos de caráter “físico” que, no passado, tornavam impossíveis ou extremamente difíceis os acessos à distância, múltiplos. (RODOTÁ, 2008, p. 69)

Observa-se assim que a revolução tecnológica não é um fenômeno acabado, mas sim um processo submetido a constantes e relevantes transformações, difundindo-se nos mais diversos âmbitos. Apesar dos benefícios trazidos pela tecnologia, é importante frisar que a facilidade de acesso traz consigo diversos riscos a outros direitos fundamentais, entre eles o direito à privacidade, levando ao surgimento de uma sociedade de vigilância, o que será analisado a seguir.

3 – ESTADO DE VIGILÂNCIA E SEGURANÇA

Na sociedade da informação, todo e qualquer uso da rede deixa um rastro de dados do usuário, cada vez mais a informação está contida no meio eletrônico, principal meio de retenção dos dados pessoais.

A utilização do *big data* é cada vez mais presente na sociedade da informação, atingindo todas as práticas humanas, ocorram elas em sistemas informatizados ou não. Nesse sistema, trabalha-se com os dados em larga escala, armazenando-os com a finalidade de transformar esses dados em informações[18], possibilitando a antecipação de tendências e criando perfis.

Chegou-se a um ponto tal em que já existem locais, como a Coreia do Sul[19], onde a maior parte da vida social ocorre de forma eletrônica. Segundo Eugène Enriquez (2004, p. 49), “aqueles que prezam sua invisibilidade tendem a ser rejeitados, postos de lado ou transformados em suspeitos de um crime”, ou seja, nessas culturas não há verdadeira escolha, mas sim uma necessidade de seguir pelo caminho da exposição.

Daí surge o conflito explanado por Stefano Rodotá (2008, p. 137):

> A tutela das informações pessoais revela-se como elemento essencial da personalidade e da cidadania: e, justamente por isso, estamos diante de uma matéria na qual não podem haver vencedores e vencidos. Da amplitude e da efetividade das garantias asseguradas à privacidade, como momento constitutivo da esfera pública e da esfera privada, depende, em grande parte, a possibilidade de que a sociedade da informação evolua para uma sociedade ‘do conhecimento e do saber’, e não para uma sociedade da vigilância, da classificação e do controle.

Não se sabe em que direção a sociedade da informação seguirá. Na opinião de Zygmunt Bauman (2014, p. 97), a sociedade está em um estado de “servidão voluntária”, cooperando com a vigilância eletrônica em uma tentativa de escapar ao abandono e à solidão por meio das redes sociais, que nos conectam a todo o mundo.

Inclusive, é esse o maior apelo das redes sociais, a possibilidade de conectar diversos subgrupos de amigos, construindo uma só comunidade onde todos se

---

18 A informação organiza os dados disponíveis e, assim, adquire utilidade. Os dados seriam uma “pré informação”.

19 Destaque-se que, segundo o Internet World Stats, 96% da população sul-coreana tem acesso à Internet, um dos maiores índices do mundo

conhecem. Conforme lição de Bauman (2014, p. 33), “o advento de uma ‘aldeia global’, parece ter se tornado realidade, ainda que virtualmente”.

Além disso, não se pode esquecer que a maioria dos dados disponíveis na internet tem como origem os próprios indivíduos, que os cedem tanto por necessidade (para ter acesso a certos bens ou benefícios) quanto voluntariamente através de redes sociais ou outras ferramentas de interação social. Bauman (2014, p. 20) inclusive aponta que, de certa forma, “submetemos à matança nossos direitos de privacidade por vontade própria”.

Segundo Stefano Rodotá (2008, p. 113):

> A contrapartida necessária para se obter um bem ou um serviço não se limita mais à soma de dinheiro solicitada, mas é necessariamente acompanhada por uma cessão de informações. Nessa troca, então, não é mais somente o patrimônio de uma pessoa que está envolvido. A pessoa é obrigada a expor seu próprio eu, sua própria persona, com consequências que vão além da simples operação econômica e criam uma espécie de posse permanente da pessoa por parte de quem detém as informações a seu respeito.

Ou seja, entende-se que este compartilhamento desenfreado de dados – muitas vezes de natureza pessoal – é o “preço” a ser pago para integrar a sociedade da informação. Rompe-se o sigilo, fronteira da privacidade, como “espaço daquilo que é do domínio da própria pessoa, o território de sua soberania total” (BAUMAN, 2014, p. 24).

Essa é a dimensão da revolução tecnológica e da globalização. A partir do momento em que a informação é colocada em um banco de dados, o indivíduo não consegue mais controlar como se dá o seu acesso e compartilhamento, muito menos excluí-la definitivamente da rede.

Junto a isso, há uma certa indiferença em relação a essa invasão na esfera da privacidade, intimamente ligada ao consumismo, o que faz com que a vigilância assuma uma faceta inofensiva.

> Obviamente, graças à minha cooperação diligente, ainda que involuntária, os servidores da Amazon agora conhecem meus hobbies ou preferências melhor do que eu. Não vejo mais suas sugestões como algo comercia; encaro-as como uma ajuda amigável, que facilita meu avanço pela selva do mercado editorial. E fico grato. E a cada nova compra, eu pago para que atualizem minhas preferências em sua base de dados e orientem minhas futuras compras com precisão. […] Com efeito, um empreendimento intencional e descaradamente restritivo, no estilo pan-óptico, é disfarçado

> como exemplo de operação sinóptica hospitaleira e socialmente amigável, sob a bandeira da solidariedade. (BAUMAN, 2014, p. 85-86)

No entanto, a liberdade infinita que aparentemente cerca a internet entra em conflito com a realidade. Câmeras de vídeo, coleta de rastros deixados pelo cartão de crédito, dados recolhidos durante a navegação na rede, interconexões entre bancos de dados, todos esses são indícios da expansão de uma sociedade onde o controle é a norma.

Segundo Rodotá (2008, p. 132), “o ingresso dos dados pessoais no mundo das mercadorias […] mudaria a própria natureza do direito à privacidade: de direito fundamental da pessoa se transformaria em título a ser negociado no mercado”, e é isto que vem ocorrendo.

Observa-se que, apesar da tutela constitucional e das diversas normas infraconstitucionais em defesa da privacidade, a população é submetida a uma vigilância contínua, tanto pelo Governo quanto por particulares, realizada com o auxílio dos mais diversos aparatos tecnológicos.

> […] o enorme aumento da quantidade de informações pessoais coletadas por instituições públicas e privadas visa sobretudo a dois objetivos: a aquisição dos elementos necessários à preparação e gestão de programas de intervenção social, por parte dos poderes públicos, e o desenvolvimento de estratégias empresariais privadas; e o controle da conformidade dos cidadãos à gestão política dominante ou aos comportamentos prevalecentes (RODOTÁ, 2008, p. 28)

Tal intromissão na esfera privada dos indivíduos é realizada sob o argumento de que a segurança coletiva é mais importante do que a preservação da proteção às informações pessoais, cada vez mais desejadas. Direitos como a dignidade e a liberdade têm sido desrespeitados em prol de uma segurança inatingível, como já havia alertado Bauman (2014, p. 81-82):

> […] vejo esse compromisso com a eficácia da técnica e da invenção – a ciência e a tecnologia de hoje – como forma de obter a paz em termos de uma falsa busca de garantia de segurança impossível de atingir. A crença de que tecnologias de segurança maiores, mais rápidas e mais conectadas possam de alguma forma garantir a paz é evidentemente equivocada e fecha as outras opções.

Eis o paradoxo da sociedade da vigilância. Mesmo sendo vigiados constantemente, os sentimentos de insegurança tornaram-se cotidianos, presentes

em todas as horas de todos os dias. Como no pan-óptico[20], a possibilidade de estar sendo observado faz com que os indivíduos se comportem como se o estivessem, e sem saber quem os observa, não têm como prever se o comportamento assumido é ou não adequado.

Constrói-se na sociedade uma estrutura baseada em um olhar que vigia e, segundo Foucault (1999, p. 226), cada um, sentindo-o pesar sobre si, terminará por interiorizá-lo ao ponto de observar-se a si mesmo; cada um assim exercerá essa vigilância sobre e contra ele mesmo. Todo o sistema eletrônico e digital é utilizado com a finalidade de vigiar, não sendo necessária a construção de um pan-óptico físico quando já existe tal versão nova e melhorada.

> Precisamos confiar na eficácia dos dispositivos de vigilância para termos o conforto de acreditar que nós, criaturas decentes que somos, escaparemos ilesos das emboscadas armadas por esses dispositivos – e que assim seremos reinvestidos e reconfirmados em nossa decência e na adequação de nossos métodos.(BAUMAN, 2014, p. 72)

Sendo assim, a sociedade da vigilância tem como um de seus principais elementos a dicotomia entre segurança e privacidade, ressaltando que

> […] a privacidade deve ser vista como “a proteção de escolhas de vida contra qualquer forma de controle público e estigma social” (L. M. Friedman), como a “reivindicação dos limites que protegem o direito de cada indivíduo a não ser simplificado, objetivado, e avaliado fora de contexto” (J. Rosen) (RODOTÁ, 2008, p. 12).

Entretanto, conforme já dispunha Bauman (2014, p. 31), “a escolha é entre segurança e liberdade: você precisa de ambas, mas não pode ter uma sem sacrificar pelo menos parte da outra”. Aparentemente, a escolha da sociedade moderna foi abdicar de parte de sua privacidade, tanto como coletividade quanto no âmbito individual, levando-a a um ponto em que a vigilância é tão eficaz que já não é possível contê-la.

Como consequência do estado de alerta contínuo que assola a sociedade, surge a “indústria de segurança”, que presta serviços de gestão de sistemas, processamento de dados pessoais, entre outros. Para se manterem nesse ramo, as empresas precisam ser cada vez mais eficientes na obtenção e análise de

20 Idealizado por Jeremy Bentham em 1785, o pan-ótico seria uma penitenciária ideal, que permite a um único vigilante observar todos os prisioneiros, sem que estes possam saber se estão ou não sendo observados, o que os leva a adotar o comportamento desejado pelo vigilante.

informações, o que implica em práticas que nem sempre respeitarão o direito à privacidade dos usuários.

Nesse sentido, Gabriela Rodríguez Fernández (2010, p. 46-47) discorre:

> Uma parte considerável dessas atividades se sustenta na capacidade de coletar, armazenar e processar dados que produzimos em nossa vida cotidiana; em muitas ocasiões, esta circunstância não é notada pelo usuário de páginas web, bibliotecas, cartões de crédito, sistemas de pagamento automático em rodovias (o "teletac") ou telefones móveis, seja porque ilegalmente não lhe é avisado ou porque se condiciona a prestação ou a rapidez do serviço à aceitação desta coleta. Os dados assim obtidos são ainda trocados entre as empresas e, em certos casos, compartilhados com a administração com fins de controle.[21]

Entretanto, mesmo a promessa de segurança revela-se, no mínimo, duvidosa, já que na sociedade da informação, onde tudo está conectado, o vazamento de dados tornou-se algo comum. No final do ano de 2019, mais de 2 milhões de usuários de câmeras de segurança da empresa Wyze tiveram seus dados vazados, incluindo informações relacionadas à saúde (HIGA, 2019).

Na violação de privacidade citada, os dados eram inseridos pelos próprios usuários no sistema, como uma "facilidade" ou "benefício" da vida moderna, e, portanto, é possível evitar ser vítima desse tipo de ataque apenas não utilizando tais ferramentas.

Infelizmente, muitas vezes o cidadão moderno deve compartilhar suas informações para ter direito a serviços básicos, inclusive governamentais, perdendo o controle sobre quem os acessa. Foi o caso de 28 mil pessoas que buscaram apoio financeiro da Secretaria de Cultura de São Paulo e tiveram seus dados expostos, inclusive RG, CPF e comprovante de endereço, por meio de uma "falha técnica" (VENTURA, 2019).

No mesmo ano, informações de quase toda a população do Equador foram expostas, abrangendo desde o número de identidade a detalhes financeiros, inclusive dados de crianças. Além disso, tais informações ficaram à disposição por um tempo relevante, sendo necessária a atuação do Centro de Respostas a

---

21 Tradução livre de: "Una parte considerable de estas actividades se sustenta en la capacidad de recoger, almacenar y procesar datos que producimos en nuestra vida cotidiana; en muchas ocasiones, esta circunstancia no es advertida por el usuario de páginas web, bibliotecas, tarjetas de crédito, sistemas de pago automáticos en autopistas (el «teletac») o teléfonos móviles, sea porque antijurídicamente no le es advertido o porque se condiciona la prestación o la rapidez del servicio a la aceptación de esta recogida. Los datos así obtenidos son además intercambiados entre las empresas y, en ciertos supuestos, compartidos con la administración a fines de control."

Incidentes em Computadores do Equador (Ecucert) para que o servidor vulnerável fosse contatado e protegido (ALECRIM, 2019).

Conclui-se, portanto, que apesar da sociedade da vigilância defender que os dados pessoais devem ser fornecidos pelo bem da coletividade, ela mesma é uma das maiores ameaças à segurança e sigilo dessas informações, sendo incapaz de protegê-los.

No entanto, essa insegurança não impede que os indivíduos forneçam seus dados pessoais, em parte por necessidade, em parte como consequência da manipulação a que foram submetidos. O próprio Bauman (2014, p. 24) já havia dito que “numa surpreendente guinada de 180 graus em relação aos hábitos de nossos ancestrais, perdemos a coragem, a energia e, acima de tudo, a disposição de persistir na defesa desses direitos [à privacidade e ao sigilo]”.

Na realidade, a segurança é apenas uma justificativa que torna mais palatável o aumento da exposição, a transparência é o verdadeiro objetivo e ideal dessa sociedade, invadindo as vidas de todos, tornando-se um imperativo, o único modo de existir.

Nesse contexto, aquele que se sente constantemente vigiado – uma das principais finalidades do modelo pan-óptico – também vigia e invade a privacidade do outro, tornando público aquilo que deveria ser privado. E esse modo de vida é aceito como normal.

Segundo Rodotá (2008, p. 157), uma das características da sociedade da vigilância é que ela aproveita todas as oportunidades que encontra para se fortalecer e permanecer viva, proliferando o medo de tal forma que o cidadão comum não apenas está disposto a entregar seus dados, mas enxerga tal exposição como a única forma de se manter seguro. De acordo com Gabriela Rodríguez Fernández (2010, p. 43):

> Estar seguro ya no es un estatus, sino un perfil que se corresponde a una actividad: comporta a la vez pertenecer al grupo de quienes pueden ser parte normalizada del mercado de consumo de bienes de seguridad —alarmas, servicios de vigilancia, GPS, etc.— y ser un sujeto que participa de las actividades que favorecen la creación de bases de datos al servicio del control —viajes en avión, uso de Internet y de telefonía móvil, tarjetas de crédito, etc.[22]

22 Estar seguro já não é um status, senão um perfil que corresponde a uma atividade: comporta tanto pertencer ao grupo das pessoas que podem ser parte normalizada do mercado de consumo de bens de segurança – alarmes, serviços de vigilância, GPS, etc. – quanto ser um sujeito que participa das atividades que favorecem a criação de bases de dados a serviço do controle –

É um sistema que se autossustenta. Ao mesmo tempo em que os dispositivos de segurança sabem onde estão os seus usuários, eles também criam necessidades – compras eletrônicas, cadastros, o próprio acesso à internet – que tornam possível obter ainda mais informações sobre eles.

Ou seja, a segurança demanda atividade, movimento, fornecer dados e comprar bens recebendo nada ou muito pouco em troca. Como dito por Rodotá, a informação é parte do valor que deve ser pago por um serviço, e ela deve ser fornecida de forma constante e sem barreiras.

> A sociedade da informação se especifica, portanto, como sociedade dos serviços, com elevada padronização e crescentes vínculos internacionais. Disso decorrem duas consequências: quanto mais os serviços são tecnologicamente sofisticados, mais os indivíduos deixam nas mãos do fornecedor do serviço uma cota relevante de informações pessoais; quanto mais a rede de serviços se alarga, mais crescem as possibilidades de interconexões entre banco de dados e de disseminação internacional das informações coletadas. (RODOTÁ, 2008, p. 66)

Em suma, nas palavras de Bauman (2014, p. 99): “A vigilância digital é uma espada afiada cuja eficácia ainda não sabemos como reduzir – e, obviamente, uma espada com dois gumes, que ainda não conseguimos manejar com segurança”.

---

viagens de avião, uso de Internet e de telefonia móvel, cartões de crédito, etc.

4 – O DIREITO NO AMBIENTE VIRTUAL

Na sociedade contemporânea, a internet é um dos principais meios de acesso à informação e de manifestação da liberdade de expressão, ambos direitos fundamentais. Essa inovação na comunicação, facilitando a interação e troca de dados, tornou possível a superação de diversos obstáculos ao ponto em que, atualmente, é quase impossível imaginar a vida sem internet.

Em contrapartida, o uso abusivo dos meios eletrônicos, levando à exposição do cotidiano e informações dos indivíduos, demonstra que o direito à intimidade e à vida privada vem sendo negligenciado, trazendo à tona a figura da internet como elemento de dominação sobre os indivíduos.

> A rápida evolução tecnológica e a globalização trouxeram novos paradigmas para a proteção de dados pessoais, transformando tanto a economia, como a vida social, sendo imprescindível que para isso haja uma circulação de dados pessoais entre os países membros, assim como entre outros países e organizações internacionais, sem que para isso se perca o nível de proteção destes dados. (PINAR MANAS, 2016, p. 51)

Ou seja, apesar de a Internet trazer vários benefícios a seus usuários, também apresenta alguns desafios reconhecidos pela comunidade jurídica, tanto em relação à aplicação do direito no ambiente virtual, quanto pelas dificuldades em regulamentá-la e controlá-la.

Como dito por Noemi Ferrigolo (2005, p. 127), “a internet não tem dono, pertence tão somente ao patrimônio do público que utiliza, através de seus computadores interligados”.

> O grande desafio para o Direito é a compreensão e o acompanhamento dessas inovações, garantindo assim a pacificação social, o desenvolvimento sustentável nessas novas relações e, acima de tudo, a manutenção do próprio Estado Democrático de Direito. Aos operadores do Direito cabe a difícil tarefa de estudar e encontrar respostas, sensatas e inteligentes, para os novos desafios advindos desse novo paradigma, fazendo com que a pessoa humana e as novas tecnologias possam coexistir dentro de uma nova concepção de mundo. (CORRÊA, 2000, p. 3-4)

No entanto, isso não significa que leis específicas para o ambiente digital são desnecessárias. Mesmo reconhecendo que a internet está “fora do raio de ação das leis nacionais”, Rodotá (2008, p. 130) é a favor da aplicação dessas normas,

trazendo também a possibilidade de realização de acordos entre os sujeitos interessados.

Afinal de contas, mesmo que não seja possível sua aplicação a todos os casos, é necessário que existam leis adaptadas ou até criadas especialmente para a era da informação, possibilitando um controle e proteção mínima dos dados compartidos.

Além disso, todos os dias surgem novas formas de coleta e tratamento de informações, possibilitadas através da utilização da tecnologia moderna e fruto do interesse das instituições públicas e privadas na obtenção de dados particulares. Como consequência da falta de controle acerca de quem tem acesso a essas informações, as empresas transnacionais muitas vezes possuem um poder equiparável ao dos Estados soberanos, consoante o pensamento de André-Jean Arnaud (2007, p. 187):

> As empresas transnacionais, transformadas agora em atores centrais da globalização das relações econômicas, escapam largamente à regulação tanto nacional quanto internacional, O direito estatal, que, em princípio, ainda detém o monopólio do direito, apresenta-se como uma estrutura cada vez mais ausente quando se trata das relações jurídicas de fato. A regulação das empresas transnacionais é feita cada vez mais a margem do direito estatal.

Nesse mundo cada vez mais complexo e sujeito às modificações trazidas pela tecnologia, é dever dos operadores do direito garantir que as finalidades das normas sejam respeitadas, mesmo que através de instrumentos diferentes daqueles que existiam quando elas foram criadas.

4.1. DIREITO DE ACESSO À INFORMAÇÃO

Como visto alhures, o direito de acesso à informação teve sua importância reconhecida já a bastante tempo. Entretanto, com as novas tecnologias o Direito tem que modificar as normas já existentes e até promover a criação de novas leis para que seja possível garantir o acesso à informação na era digital.

Nas palavras de Salete Oro Boff e Felipe da Veiga Dias (2012, p. 340), pode-se ter como ponto de partida para essa análise o entendimento de que

> O meio digital é apenas um suporte às relações humanas, não estando livre da carga axiológica constitucional, tampouco podendo ser um espaço sem legislação, em outras palavras, nesta esfera aplicam-se as mesmas regras dos demais conflitos. Isso significa que há regramentos na rede, apesar de esta ser um âmbito de grande liberdade, tal fato não significa impunidade.

Dessa forma, não deve o direito digital ser encarado como um novo âmbito do direito, pois a ele aplicam-se as mesmas regras gerais que a qualquer outro ramo, sendo necessária apenas a sua adequação à sociedade da informação e uma modificação do suporte a ser dado do real para o virtual.

Um exemplo de norma adaptada é a Lei de Responsabilidade Fiscal (Lei Complementar nº 101/2000), alterada pela Lei Complementar nº 131/2009, que mescla o elemento da transparência com as facilidades trazidas pelas internet. Esta norma determina que a sociedade tem o direito de, através dos meios eletrônicos, acessar e acompanhar informações detalhadas sobre execução orçamentária e financeira[23].

A internet traz consigo uma maior ênfase à faceta do direito à informação como "direito de busca e acesso à informação, em respeito à pluralidade informativa na formação das convicções humanas, sem permitir lesões a outros direitos fundamentais" (SOUZA, 2008, p. 102) e como direito de ser informado, ampliando-o além de sua finalidade de prestar informações.

Outro dispositivo legal relevante é o art. 3º, III, da Lei 12.527/2011, que dispõe ser diretriz destinada a assegurar esse direito fundamental a "utilização de meios de comunicação viabilizados pela tecnologia da informação". A mesma norma traz, posteriormente, como essas inovações podem ser utilizadas pelo administrador público:

> Art. 8º É dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas.
> […]
>
> § 2º Para cumprimento do disposto no caput, os órgãos e entidades públicas deverão utilizar todos os meios e instrumentos legítimos de que dispuserem, sendo obrigatória a divulgação em sítios oficiais da rede mundial de computadores (internet).

23 Disposição do art. 48, § 1º, II – liberação ao pleno conhecimento e acompanhamento da sociedade, em tempo real, de informações pormenorizadas sobre a execução orçamentária e financeira, em meios eletrônicos de acesso público

> § 3º Os sítios de que trata o § 2º deverão, na forma de regulamento, atender, entre outros, aos seguintes requisitos:
> I - conter ferramenta de pesquisa de conteúdo que permita o acesso à informação de forma objetiva, transparente, clara e em linguagem de fácil compreensão;
> II - possibilitar a gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários, tais como planilhas e texto, de modo a facilitar a análise das informações;
> […]
>
> Art. 10.
> […]
>
> § 2º Os órgãos e entidades do poder público devem viabilizar alternativa de encaminhamento de pedidos de acesso por meio de seus sítios oficiais na internet.
> […]

Em outras palavras, a Lei de Acesso à Informação buscou incluir em seus artigos algumas diretrizes a serem seguidas para proporcionar esse direito na era digital, deixando amplo espaço de manobra para que continue a regulá-lo mesmo em face das inovações tecnológicas.

Surgindo como norma com maior grau de especificidade e indo além da administração pública, no Marco Civil da Internet (Lei 12.965/2014) a liberdade de manifestação de pensamento é reforçada e a censura prévia só é permitida no caso de crimes contra a dignidade da pessoa humana.

Além disso, essa lei determina que o uso da internet no Brasil (e as leis que a regulamentarem), tem como uma de suas finalidades a promoção do acesso à informação e ao conhecimento[24].

Para melhor entendimento do significado dessa norma, é preciso analisar a amplitude do conceito de “informação”, definida pelo *The Oxford English Dictionary* (1989, p. 944-946) como coisa, como processo e como conhecimento.

> 1. Informação como processo existe quando alguém é informado sobre aquilo que eles sabem que está sendo mudado. Nesse sentido, informação é o ato de informar, comunicar o conhecimento ou novidades de algum fato ou ocorrência; a ação de contar ou fato de estar contando algo.[25]
> 2. Informação como conhecimento. Informação é usada para simbolizar a percepção da informação como processo: o conhecimento comunicado referente a algum fato particular, sujeito ou evento; que algo é informado ou contado; inteligência, notícias. A noção de informação, desse modo, reduz a

24 Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção: […] II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;

25 Tradução livre de: “1. Information-as-process: When someone is informed, what they know is changed. In this sense ‘information’ is ‘The act of informing...; communication of the knowledge or ‘news’ of some fact or occurrence; the action of telling or fact of being told of something.”

> incerteza e pode ser vista como um caso especial de “informação como conhecimento”. Algumas vezes aumenta incertezas.[26]
> 3. Informação como coisa. O termo “informação” é também utilizado atributivamente para objetos, tais como dados e documentos, que são referidos como “informação” porque eles estão relacionados a ser informados, tal como ter a qualidade de proporcionar conhecimento informação de comunicação; instrutivo. [27]

O conhecimento é o sentido e o significado que cada pessoa atribui a uma informação como coisa. Sendo assim, para que ambos os direitos sejam garantidos é necessário que os cidadãos tenham acesso à grande massa de dados produzidos tanto por ele quanto sobre ele, além de também poder usufruir daquelas informações que façam sentido para si e o autodeterminem como ser humano.

Em face de sua importância para o desenvolvimento de qualquer sociedade moderna, inclusive a brasileira, o alcance do direito de acesso à informação já foi inclusive questionado em sede de Recurso Especial, confrontando-o com outras garantias privilegiadas do ordenamento:

> “EMENTA: AGRAVO DE INSTRUMENTO – AÇÃO DE OBRIGAÇÃO DE FAZER – PEDIDO DE ANTECIPAÇÃO DE TUTELA PARA EXCLUSÃO DE RECLAMAÇÕES REFERENTES À SOCIEDADE EMPRESÁRIA – NÃO CABIMENTO – PROVEDOR DE PESQUISA – RESTRIÇÃO DOS RESULTADOS – IMPOSSIBILIDADE – CONTEÚDO PÚBLICO – DIREITO À INFORMAÇÃO – PRECEDENTES – LEI No 12.965/2014 (MARCO CIVIL DA INTERNET) – DECISÃO MANTIDA. – [...] 7. Não se pode, sob o pretexto de dificultar a propagação de conteúdo ilícito ou ofensivo na web, reprimir o direito da coletividade à informação. Sopesados os direitos envolvidos e o risco potencial de violação de cada um deles, o fiel da balança deve pender para a garantia da liberdade de informação assegurada pelo art. 220, § 1º, da CF/88, sobretudo considerando que a Internet representa, hoje, importante veículo de comunicação social de massa.”(REsp 1316921/RJ, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 26-6-2012, DJe 29-6-2012).

Portanto, de acordo com essa decisão, os provedores de pesquisa não podem ser obrigados a eliminar do seu sistema os resultados derivados da busca de determinado termo ou expressão, considerando que eles apenas espelham o conteúdo que já existe na internet.

---

26 Tradução livre de: “2. Information-as-knowledge: ‘Information’ is also used to denote that which is perceived in ‘information-as-process’: the ‘knowledge communicated concerning some particular fact, subject, or event; that of which one is apprised or told; intelligence, news.’ The notion of information as that which reduces uncertainty could be viewed as a special case of ‘information-as-knowledge’. Sometimes information increases uncertainty.”

27 Tradução livre de: “3. Information-as-thing: The term ‘information’ is also used attributively for objects, such as data and documents, that are referred to as ‘information’ because they are regarded as being informative, as ‘having the quality of imparting knowledge or communicating information; instructive.”

Ademais, a adoção de posturas excessivamente restritivas e punitivas a informações levaria a um retrocesso no processo de acesso informativo virtual, culminando na diminuição da inserção virtual dos indivíduos, que passariam a entender a sociedade da informação como uma sociedade de risco[28]. Haveria assim a transmutação do processo progressivo da sociedade da informação na proliferação da desinformação.

Para evitar esse desfecho, “pleiteia-se o uso da rede de forma responsável, […] ponderando de maneira mais adequada quais são os verdadeiros valores que devem ser protegidos, na busca de uma maior inclusão digital e social do cidadão” (BOFF; DIAS, 2012, p. 341).

Entretanto, apesar da importância latente do direito de acesso à informação, é importante frisar que esse direito fundamental deve ser garantido em harmonia com o direito à privacidade do usuário, cada vez mais frágil na era digital, tema que será estudado a seguir.

4.2. DIREITO À PRIVACIDADE E DIREITO AO ESQUECIMENTO

Na sociedade da informação o direito à privacidade é o direito à autodeterminação informativa, que traz consigo a necessidade dos indivíduos de controlarem o fluxo e disponibilização de dados, especialmente aqueles relativos a si mesmos.

Entretanto, esse direito entra em conflito com as demandas da modernidade, onde o mero uso de aparelhos eletrônicos já implica na coleta de dados que, a partir daí, saem do âmbito de controle individual. Esse impasse é explorado por Renato Monteiro (2014, p. 141):

> Infelizmente, o registro e a guarda de logs de acesso à internet e de navegação dos usuários ainda são necessários. Essa afirmação é uma realidade principalmente para as empresas que provêm serviços de aplicação na grande rede por um grande e importante motivo: o modelo de negócio sob o qual elas estão baseadas depende quase que exclusivamente da monetização de dados dos seus usuários. Dados estes que na sua maioria são pessoais. Uma vez que a receita das empresas se origina principalmente da publicidade oferecida através de suas plataformas,

28 A sociedade de risco encontra-se associada a fenômenos econômicos após a metade do século XX, trazendo consigo a doutrina do medo, muitas vezes de “inimigos” ou ameaças invisíveis (AUGUSTIN; LIMA, 2009, p. 118)

> e a eficiência dessas propagandas está diretamente ligada à análise do comportamento dos usuários, caso estas empresas não coletassem dados, elas simplesmente não existiriam. Podemos, portanto, partir de uma premissa: com regulação estatal ou não, dados continuarão a ser coletados e armazenados, pois o atual modelo de negócio das empresas de internet depende dessa prática.

Obviamente, isso não significa que a regulação estatal é inútil – e portanto sequer deveria existir –, mas sim que esta não deve almejar o controle total do que ocorre na internet, a que muitos se referem como “terra de ninguém”, justamente por este ser impossível.

Afinal de contas, as garantias individuais ainda estão presentes e algumas delas, inclusive, recebem novo fôlego na sociedade da informação, como é o caso do direito ao esquecimento. Em relação a este, deve-se considerar que a rede mundial de computadores é uma ferramenta extremamente poderosa capaz de disponibilizar com facilidade e rapidez um conteúdo praticamente infinito, armazenado em servidores espalhados ao redor do mundo. Diante disso, na prática, é impossível garantir plenamente o direito ao esquecimento frente às transformações tecnológicas.

Esta problemática é enfatizada pelo Ministro Luís Felipe Salomão, na sede do REsp 1.334.097-RJ, já citado anteriormente:

> […] em recente palestra proferida na Universidade de Nova York, o alto executivo da Google Eric Schmidt afirmou que a internet precisa de um botão de delete. Informações relativas ao passado distante de uma pessoa podem assombrá-la para sempre, causando entraves, inclusive, em sua vida profissional, como no exemplo dado na ocasião, de um jovem que cometeu um crime em relação ao qual as informações seriam expurgadas de seu registro na fase adulta, mas que o mencionado crime poderia permanecer on-line, impedindo a pessoa de conseguir emprego.

Como forma de solucionar essa questão, o Superior Tribunal de Justiça entendeu, no julgamento do REsp 1.660.168/RJ, pelo direito à desindexação no âmbito da internet, promovendo a retirada de conteúdos ofensivos relativos a dados do passado da pessoa.

A desindexação consiste no rompimento do vínculo criado, nos bancos de dados dos provedores de busca (*Google*, *Bing*, *Yahoo*), entre dados pessoais e resultados da busca, seja pelo conteúdo eminentemente privado da informação, seja pelo decurso do tempo. O objetivo dessa intervenção é, assim como em outros casos que envolvem o direito ao esquecimento, permitir que as pessoas envolvidas

sigam suas vidas com certo anonimato, não sendo o acontecimento desagradável rememorado continuamente pelos mecanismos automatizados dos sistemas de busca.

Destaque-se que a desindexação realiza o rompimento do referido vínculo, não a exclusão da notícia. Ou seja, é possível a sua localização quando os termos utilizados na pesquisa estão relacionados ao fato noticiado, mas esta não será discriminada nos resultados quando a busca refere-se exclusivamente aos dados pessoais do indivíduo protegido. Dessa forma, o direito à desindexação no âmbito da internet compatibiliza os interesses individual do titular dos dados pessoais e coletivo de acesso à informação.

Apesar dos esforços dos Tribunais Superiores em garantir a privacidade na era da informação, logo se percebe que é inviável depender deles quando se trata de um direito tão amplo e com tantas ramificações. Consequentemente, surge a necessidade de criar normas específicas para a proteção de dados pessoais, que serão analisadas a seguir.

5 – PROTEÇÃO DE DADOS PESSOAIS

Com a globalização, surgiram novos paradigmas para a proteção de dados pessoais em todo o mundo, influenciando todos os aspectos da vida em sociedade. Em face da inevitável circulação de informações entre países e entre estes e organizações internacionais, evidenciou-se a necessidade de haver algum controle normativo que permitisse a proteção destes dados.

Além disso, a Carta Europeia de Direitos Humanos reconhece, em seu artigo 8º, a proteção de dados como direito fundamental autônomo, separado do direito à intimidade.

> Artigo 8º.
> Protecção de dados pessoais
> 1. Todas as pessoas têm direito à protecção dos dados de caráter pessoal que lhes digam respeito.
> 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.
> 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente. (UNIÃO EUROPEIA, 2000)

Nesse contexto, surgem diversas normatizações, especialmente na Europa, buscando regular o direito à proteção de dados pessoais, como as Diretivas 95/46/CE e 2002/58/CE do Parlamento Europeu e do Conselho da Europa, que, apesar de apresentarem problemas em sua aplicação, tiveram um papel fundamental como pioneiras do tema.

A normatização europeia mais recente é o Regulamento Geral sobre a Proteção de Dados (RGPD) 2016/679, implementado em 25 de maio de 2018, cujo objetivo é dar aos cidadãos e residentes da União Europeia e do Espaço Econômico Europeu formas de controlar os seus dados pessoais, ao mesmo tempo em que unifica o quadro regulamentar europeu.

É importante frisar que, diferentemente das normas anteriores, o RGPD é um regulamento, e não uma diretiva[29], tornando-o vinculativo e aplicável sem necessidade de aprovação de legislação adicional por parte dos estados-membro.

---

29 Ato legislativo da União Europeia que exige que os Estados-membros alcancem um determinado resultado, sem determinar os meios através dos quais deverão alcançá-lo, dando-lhes uma certa dose de flexibilidade.

O RGPD tem como base a noção de que o tratamento de dados pessoais é um serviço à humanidade, devendo tal direito ser considerado no contexto da coletividade, mantendo-se em equilíbrio com os demais direitos fundamentais, baseado em certos princípios.

5.1. PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Inicialmente, a privacidade e a intimidade estão garantidas no art. 5º, incisos X e XII, da Constituição. Com base nisso, diversas normas surgiram ao longo dos anos objetivando a garantia desses direitos fundamentais, sendo o Marco Civil da Internet (Lei 12.965/2014) uma das que trouxeram normas aplicáveis ao contexto da sociedade da informação.

Ao longo dos últimos anos, a legislação brasileira tem seguido o caminho traçado pelas normas internacionais, dando maior ênfase ao direito ao sigilo de dados e à autodeterminação informacional.

Em convergência com a legislação europeia e também por conta de pressões políticas – uma legislação sobre proteção de dados pessoais é uma exigência para ingresso na Organização para a Cooperação e Desenvolvimento Econômico (OCDE) –, foi criada a Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD).

Esta norma dispõe expressamente sobre o tratamento de dados pessoais em qualquer mídia, não se aplicando somente aos meios digitais, o que amplia sua incidência e adaptabilidade, sendo considerado dado pessoal, para os fins da lei, a informação relacionada a pessoa natural identificada ou identificável[30].

Além disso, a nova lei regula também as empresas domiciliadas no exterior sempre que os dados pessoais tenham sido coletados em território nacional ou o seu tratamento ocorra no Brasil. Dessa forma, abrange uma maior quantidade de corporações, possibilitando assim uma melhor proteção aos direitos fundamentais de liberdade e privacidade.

Em seu artigo 6º, a Lei Geral de Proteção de Dados Pessoais traz quais são os princípios que, junto à boa-fé, deverão ser observados durante as atividades de

30 Disposição do Art. 5º, I

tratamento de dados pessoais, sendo as demais normas decorrência da aplicação direta ou indireta desses princípios, que costumam estar interligados.

5.1.1. PRINCÍPIOS DA FINALIDADE, ADEQUAÇÃO E NÃO DISCRIMINAÇÃO

O princípio da finalidade trazido pelo Art. 6º, I, da LGPD[31] tem suas raízes na boa fé objetiva conforme prevista na Diretiva 95/46/CE. A boa fé objetiva tem como principal função estabelecer uma conduta ética, leal e honesta de todas as partes de uma relação jurídica, sendo esse um dos princípios basilares do direito e fonte de equilíbrio.

> Artigo 6º
> 1. Os Estados-membros devem estabelecer que os dados pessoais serão:
> a) Objecto de um tratamento leal e lícito;
> b) Recolhidos para finalidades determinadas, explícitas e legítimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades. O tratamento posterior para fins históricos, estatísticos ou científicos não é considerado incompatível desde que os Estados-membros estabeleçam garantias adequadas. (UNIÃO EUROPEIA, 1995)

Ou seja, os dados devem ser recolhidos somente se autorizados pelo respectivo titular[32], que deve ter conhecimento de como eles serão utilizados, possibilitando assim que o indivíduo controle-os e seja capaz de tomar uma decisão informada.

Como complemento da finalidade, está previsto na norma o princípio da não discriminação[33], que veda a coleta e uso de dados se o objetivo de tal tratamento é ilícito ou abusivo, limitando os poderes do controlador e do operador.

> Lei 13.709/2018
> […]
>
> Art. 5º Para os fins desta Lei, considera-se:
> […]

31 Art. 6º, I: “finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.”

32 Essa é a disposição do Art. 7º, I: “O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I – mediante o fornecimento de consentimento pelo titular;”

33 Art. 6º, IX: “não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;”

> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
>
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Outra restrição a sua autoridade surge como consequência do princípio da adequação[34], onde está determinado que o uso das informações obtidas deve se dar conforme aquilo que foi informado ao indivíduo, não podendo ser utilizadas para fim diverso daquele para o qual foram fornecidas.

Além disso, é importante frisar que a Lei Geral de Proteção de Dados garantiu ao titular um maior controle também sobre a transmissão de seus dados, retirando-o da posição de escravo desse tratamento. Mesmo que o indivíduo tenha autorizado a coleta, é necessário obter consentimento específico para a comunicação ou compartilhamento dessas informações[35].

No entanto, a depender dos objetivos da coleta e uso dos dados pessoais, não será aplicada a LGPD, embora os seus princípios continuem servindo como guia para realização do tratamento das informações.

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> […]
>
> II - realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
>
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> […]
>
> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

34 Art. 6º, II: “adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;”

35 Art. 7º, §5º: “O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.”

5.1.2. PRINCÍPIO DA NECESSIDADE

Em um contexto geral, o princípio da necessidade[36] assemelha-se à proporcionalidade, cujo principal objetivo é garantir o equilíbrio entre os direitos e liberdades individuais e os anseios da coletividade, eis que não existe nenhum direito que seja absoluto, capaz de suprimir quaisquer outras garantias para concretizar-se.

No que se refere a proteção de dados pessoais, a necessidade serve como parâmetro para a exclusão do tratamento de informações não pertinentes à atividade desenvolvida. Um exemplo de sua aplicação, segundo Pablo Pallazzi (2002, p. 176-177), é o fato de que não é possível armazenar dados relativos a obrigações econômicas ou financeiras se tais informações não são essenciais às finalidades da coleta ou referem-se a dívidas já quitadas.

> 1.Os Estados-membros devem estabelecer que os dados pessoais serão (…)
>
> b) Recolhidos para finalidades determinadas, explícitas e legítimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades. (…)
>
> c) Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente (UNIÃO EUROPEIA, 1995)

Em decorrência desse princípio surge o direito de oposição, ou seja, a faculdade de o indivíduo opor-se à coleta de seus dados pessoais caso lhe sejam solicitados dados inadequados, desnecessários ou desproporcionais aos fins almejados. É uma consequência do direito individual de controlar o tratamento de suas informações pessoais.

Sendo assim, a oposição abrange não apenas o direito de negar qualquer pedido de informação, mas também o direito de opor-se ao tratamento de seus dados pessoais caso estes tenham sido fornecidos por terceiros.

> Artigo 14º
> Direito de oposição da pessoa em causa
> Os Estados-membros reconhecerão à pessoa em causa o direito de:

36 Art. 6º, III: “necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;”

> a) Pelo menos nos casos referidos nas alíneas e) e f) do artigo 7º, se opor em qualquer altura, por razões preponderantes e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objecto de tratamento, salvo disposição em contrário do direito nacional. Em caso de oposição justificada, o tratamento efectuado pelo responsável deixa de poder incidir sobre esses dados; (UNIÃO EUROPEIA, 1995)

Tal direito somente poderá ser negado em casos excepcionais, como quando a coleta é imposta por dispositivo legal, a exemplo do fornecimento de informações ao poder público para efeitos fiscais; ou quando houver a necessidade de prestação da informação para preservação de interesse público, como em situação de segurança pública ou combate e prevenção a epidemias[37].

Entretanto, mesmo quando é dispensado o consentimento do titular, o tratamento de dados deve ser realizado em observância aos princípios gerais e às obrigações previstas na LGPD, podendo o titular opor-se a ele se houver descumprimento das normas[38].

Já quando a solicitação de informações pessoais for considerada desproporcional, inadequada ou desnecessária ao cumprimento das finalidades propostas pela coleta, o indivíduo poderá negar tal pedido, tendo assim preservada a sua privacidade.

5.1.3. PRINCÍPIOS DA TRANSPARÊNCIA, LIVRE ACESSO E QUALIDADE DOS DADOS

Tais princípios, previstos no art. 6º da Lei Geral de Proteção de Dados, têm como principal finalidade a defesa e preservação das garantias individuais exploradas anteriormente, permitindo a moderação eficaz da coleta e do uso de dados, inclusive em relação ao cumprimento dos fundamentos previstos nessa mesma norma.

O princípio da transparência[39] prevê que o titular tenha conhecimento de como se dará o tratamento das informações fornecidas, ou seja, qual a sua

37 Conforme disposição do Art. 7º, II e III
38 Segundo o artigo 18, §2º
39 Art. 6º, VI: “transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;”

finalidade, por quanto tempo os dados serão conservados, entre outros, possibilitando assim o exercício dos seus direitos.

Inicialmente, o indivíduo deve ser notificado da coleta dos dados pessoais e, se preciso, nesse momento será obtida a sua autorização para tal recolhimento. Havendo necessidade de utilizar esses dados para outras finalidades além daquelas definidas anteriormente ou transmiti-los a terceiros, é essencial informar tal mudança ao titular dos dados (CASTRO, 2005, p. 244).

> a obrigação de informar os assinantes do fim ou fins a que se destinam as listas públicas em que vão ser incluídos os seus dados pessoais deverá caber à parte que recolhe os dados tendo em vista essa inclusão. Nos casos em que os dados pessoais possam ser transmitidos a um ou mais terceiros, o assinante deverá ser informado desta possibilidade e do destinatário (…) (UNIÃO EUROPEIA, 2002)

Segundo Pablo Pallazzi (2002, p. 229), somente é possível dispensar o consentimento expresso quando a coleta deriva de uma relação contratual firmada; quando esta é exercida pelo Estado; ou quando os referidos dados são obtidos através de fontes de acesso público irrestrito.

Esse princípio é violado quando ocorre a coleta não autorizada e a realizada de forma oculta por meio de *cookies*[40], *spywares*[41], *keyloggers*[42], entre outros dispositivos de monitoramento eletrônico. Tais práticas afrontam também o direito à informação, visto que o titular dos dados perde o controle sobre seus dados pessoais.

Como consequência da transparência, há o princípio do livre acesso[43], que possibilita ao titular o conhecimento quanto a seus dados, sendo que tal informação deve ser prestada em prazo razoável, de forma inteligível e, via de regra, sem necessidade de apresentação de justificativas[44].

---

40 *Cookies* são arquivos que armazenam temporariamente o que o internauta está visitando na rede. Por não haver limite para quais informações eles podem armazenar, incluindo login, senhas e histórico de navegação, cria-se um risco de exposição da privacidade do usuário

41 É um *software* (programa) espião de computador cujo objetivo é observar e roubar informações pessoais do usuário, retransmitido-as para uma fonte externa na internet. Isso é feito sem o conhecimento ou consentimento do internauta

42 Programa do tipo *spyware* criado para gravar tudo que o usuário digita no teclado de um computador, frequentemente utilizado para capturar dados bancários, senhas e outros tipos de dados pessoais

43 Art. 6º, IV: “livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;”

44 O direito de acesso do titular está regulamentado de forma mais detalhada no artigo 9º da LGPD, que dispõe acerca da abrangência desse direito, que informações devem ser disponibilizadas, entre outros.

O acesso à informação está previsto tanto na Lei nº 12.527/2011, já explorada anteriormente, quanto na Lei nº 9.507/97 (Lei do *Habeas Data*). Esta última também admite a concessão desse remédio constitucional para a retificação da informação, relacionando-se assim ao princípio da qualidade dos dados[45], cujo fundamento assemelha-se à veracidade prevista na Directiva 95/46/CE.

> Artigo 6º
> 1. Os Estados-membros devem estabelecer que os dados pessoais serão:
> […]
>
> d) Exactos e, se necessário, actualizados; devem ser tomadas todas as medidas razoáveis para assegurar que os dados inexactos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente, sejam apagados ou rectificados; (UNIÃO EUROPEIA, 1995)

Também conhecido como princípio da exatidão e atualização dos dados, seu principal objetivo é garantir ao seu titular o direito de corrigir informações incorretas ou alterar dados desatualizados, visto que tais erros têm o potencial de causar sérios prejuízos ao indivíduo.

5.1.4. PRINCÍPIOS DA SEGURANÇA, PREVENÇÃO E RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS

Estes princípios são, dentre os previstos na Lei Geral de Proteção de Dados, os mais direcionados aos deveres que devem ser cumpridos pelos agentes que realizam o tratamento de dados, buscando garantir os direitos conferidos aos seus titulares tanto nessa lei quanto em qualquer outra parte do ordenamento jurídico.

A segurança no tratamento de dados[46] tem sido fonte de grande preocupação desde as primeiras normas acerca da proteção de dados pessoais. A Directiva 95/46/CE, por exemplo, já dispunha que:

---

45 Art. 6º, V: "qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;"

46 Art. 6º, VII: "segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;"

> Artigo 17º Segurança do tratamento
> 1. Os Estados-membros estabelecerão que o responsável pelo tratamento deve pôr em prática medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou acesso não autorizados […]. Estas medidas devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger.

A adoção de medidas de segurança é um requisito essencial para a realização do tratamento de dados pessoais, visto que essa é uma atividade de risco, especialmente em face do exponencial desenvolvimento tecnológico ao longo dos últimos anos.

O princípio da segurança está intimamente associado à prevenção[47], podendo ser considerada uma das formas de exercício desta. Entretanto, eles não devem ser confundidos, pois é possível que ocorram danos sem violação às medidas de proteção, quando, por exemplo, os dados estão desatualizados ou confusos.

Por fim, a responsabilização e prestação de contas[48] é um princípio que, em termos gerais, determina que as medidas adotadas com o objetivo de garantir a proteção de dados pessoais devem ser aptas à realização dessa finalidade, sendo dever do agente que as adota comprovar tal eficácia.

47 Art. 6º, VIII: “prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;”

48 Art. 6º, X: “responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.”

CONSIDERAÇÕES FINAIS

O presente trabalho inicia sua narrativa na Revolução Industrial, onde surge a noção inicial de privacidade e, posteriormente, o seu reconhecimento como direito no artigo “The Right to Privacy”. Apesar de diversos estudiosos tentarem defini-lo, a indeterminação do conceito desse direito é uma de suas ferramentas de proteção mais poderosas, permitindo que adapte-se com maior facilidade aos diferentes contextos em que tal a privacidade deve ser preservada.

Na sociedade moderna, o direito fundamental à intimidade é relacionado à dignidade da pessoa humana e, portanto, parte essencial de qualquer Constituição, inclusive a brasileira. Quando da análise de sua proteção infraconstitucional e da jurisprudência dos tribunais superiores, percebeu-se que estas costumam ser voltadas ao direito à indenização.

Diversamente, a garantia do direito ao esquecimento costuma, por sua própria natureza, levar à aplicação de medidas punitivas além da reparação, já que seu principal objetivo é evitar que um fato da vida do indivíduo continue a atormentá-lo mesmo quando não mais houver interesse atual por ele. São citados como exemplos o caso Lebach e a Chacina da Candelária.

O primeiro tópico encerra-se com a análise do direito à privacidade na sociedade globalizada, enfatizando-se a relativização de sua inviolabilidade e as mudanças ocorridas em seu conceito. Na modernidade, há um maior interesse na possibilidade de controle do fluxo e disponibilização de informações do que no “direito de ser deixado só” que a caracteriza em sua origem.

Prossegue-se então para o estudo do direito à informação, cujo acesso expandiu-se através de diversos pontos de virada na história, a exemplo do surgimento da Imprensa de Gutenberg. Apesar de ter sido reconhecido como garantia na Suécia em 1776, onde foi promulgada a primeira lei nesse sentido, somente em 1948 o direito de acesso à informação foi reconhecido internacionalmente, passo fundamental para sua consolidação como direito fundamental no ano 2000.

Logo após, realizou-se uma breve exposição dos principais pontos trazidos pela Lei nº 12.527/2011 (Lei de Acesso à Informação), onde houve a regulamentação dos procedimentos a serem adotados não só para a concretização

desse direito, mas também para garantir a transparência de gerenciamento e veracidade dos dados obtidos.

As transformações nos meios de comunicação sempre influenciaram o acesso à informação, e com a revolução tecnológica não foi diferente. A internet se incorporou rapidamente à vida moderna, criando formas de correspondência e interação caracterizadas por sua larga escala, promovendo o acesso em proporções nunca antes vistas.

Entretanto, o tópico seguinte explora como a grande circulação de informações apresenta alguns riscos a outros direitos fundamentais, cujo extremo seria o surgimento de uma sociedade de vigilância.

Nesse Estado, o compartilhamento de dados pessoas e a vigilância contínua são vistos como algo natural; a invasão da esfera privada é justificada como um meio para garantir a segurança coletiva. Logo se observa que essa promessa não passa de mera falácia, já que o vazamento de dados é um fenômeno relativamente comum na sociedade da informação, conforme os exemplos trazidos ao longo desse trabalho.

Inicia-se então uma discussão acerca de como o Direito pode atuar no âmbito da internet, contexto bastante diferente daquele para o qual foi elaborado. A princípio, foi estabelecido que almejar o controle absoluto é inviável, devendo-se ter como objetivo, ao invés disso, uma proteção mínima dos dados e de seus titulares.

Foi analisado então o direito à informação, cuja faceta de direito de busca e acesso é posta em evidência com o advento das novas tecnologias, sendo essa uma das finalidades da internet de acordo com o Marco Civil da Internet (Lei nº 12.965/2014). Para garantir uma melhor efetivação, defende-se o uso responsável da rede, sem necessidade de adoção de medidas excessivamente restritivas, tendo em vista o potencial que possuem de prejudicar a inclusão digital.

Em seguida, foram abordadas as particularidades do direito à privacidade na modernidade como direito à autodeterminação informativa, ao controle do fluxo de dados, em especial na forma de direito à desindexação. Este é trazido como um excelente exemplo de compatibilização entre os interesses individual (privacidade) e coletivo (acesso à informação).

Por fim, observou-se que, da necessidade de caminhos designados especificamente para a proteção de dados pessoais, surgiram diversas normas, sendo pioneiras no tema as Diretivas do Parlamento Europeu e do Conselho da

Europa. No entanto, apenas recentemente o Brasil desenvolveu uma legislação especial própria, na forma da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018).

Os princípios que a regem prezam, em especial, por um tratamento de dados que respeite o titular, realizado nos limites de seu consentimento e em proporção bastante apenas para a satisfação das finalidades apresentadas, preservando assim suas garantias individuais. Alguns dos princípios, inclusive, são direcionados aos agentes, orientando-os à essencialidade da segurança no exercício de sua atividade.

Ante todo o exposto, é notável a importância de serem trabalhadas alternativas para a proteção do direito à privacidade no âmbito virtual, seja por meio da criação de novas leis, seja pela adaptação de normas já vigentes, como demonstrado no decorrer desse trabalho. Apesar da vitória representada pela Lei Geral de Proteção de Dados, sua mera existência não basta, por si só, para garantir sua eterna eficácia como meio de defesa da intimidade.

Portanto, é necessário que a LGPD, as instituições que a acompanham e as normas esparsas sobre o tema sejam vistas de forma crítica e sugestiva, sendo aperfeiçoadas ao longo dos anos, adaptando-se ao irrefreável desenvolvimento tecnológico. Dessa forma, a longo prazo, essa estrutura será capaz de concretizar uma segurança jurídica ampla e atual nos meios digitais.

REFERÊNCIAS

ALECRIM, Emerson. Vazamento pode ter exposto dados de quase toda a população do Equador. **Tecnoblog**, 17 set. 2019. Disponível em: https://tecnoblog.net/307316/vazamento-dados-20-milhoes-cidadaos-equador/. Acesso em 06 set. 2020.

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Tradução: Virgílio Afonso da Silva. São Paulo: Malheiros, 2008.

ARNAUD, André-Jean. **Governar sem fronteiras**. Rio de Janeiro: Editora Lumens Juris, 2007.

ASCENSÃO, José de Oliveira, **Direito da Internet e da sociedade da informação**. Rio de Janeiro: Forense, 2002.

AUGUSTIN, Sérgio; LIMA, Letícia Gonçalves Dias. O controle jurisdicional da discricionariedade técnica e os conceitos indeterminados na sociedade de risco: o elemento coletivo na nova responsabilidade ambiental. *In*: SPAREMBERGER, Raquel Fabiana Lopes; AUGUSTIN, Sérgio (org.). **O direito na sociedade de risco**: dilemas e desafios socioambientais. Caxias do Sul: Plenum, 2009.

BARROSO, Luís Roberto. Liberdade de expressão versus direitos da personalidade. Colisão de direitos fundamentais e critérios de ponderação. *In*: SARLET, Ingo Wolfgang (org.). **Direitos fundamentais, informática e comunicação**: algumas aproximações. Porto Alegre: Livraria do Advogado, 2007, p. 63-100.

BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. **Comentários à Constituição do Brasil**. São Paulo: Saraiva, 1989, vol. 2.

BAUMAN, Zygmunt; LYON, David. **Vigilância Líquida**. Tradução: Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2014.

BOBBIO, Norberto. Democracia e Segredo. *In*: BOVERO, Michelangelo (Org.). **Teoria Geral da Política**: A Filosofia Política e as Lições dos Clássicos. Rio de Janeiro: Elsevier, 2000.

BOFF, Salete Oro; DIAS, Felipe da Veiga. O Acesso à Informação no Campo Digital: Uma Análise entre a Sociedade da Informação e a Sociedade de Risco. **Revista de Estudos Jurídicos UNESP**, São Paulo, a.16, n. 23, p. 329-344, 2012.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 06 set. 2020.

BRASIL. **Lei Complementar nº 101, de 4 de maio de 2000**. Estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal e dá outras providências. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp101.htm. Acesso em 06 set. 2020.

BRASIL. **Lei nº 11.111, de 5 de maio de 2005**. Regulamenta a parte final do disposto no inciso XXXIII do caput do art. 5º da Constituição Federal e dá outras providências. Brasília, DF: Presidência da República, [2005]. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Lei/L11111impressao.htm. Acesso em 06 set. 2020.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, [2011]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em 06 set. 2020.

BRASIL. **Lei nº 12.528, de 18 de novembro de 2011**. Cria a Comissão Nacional da Verdade no âmbito da Casa Civil da Presidência da República. Brasília, DF: Presidência da República, [2013]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12528.htm. Acesso em 06 set. 2020.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da

República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 06 set. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em 06 set. 2020.

BRASIL. **Lei nº 8.159, de 8 de janeiro de 1991**. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Brasília, DF: Presidência da República, [1991]. Disponível em: https://www2.camara.leg.br/legin/fed/lei/1991/lei-8159-8-janeiro-1991-322180-norma-pl.html. Acesso em 06 set. 2020.

BRASIL. Superior Tribunal de Justiça (3ª turma). **Recurso Especial 1.316.921-RJ (2011/0307909/6)**. Recorrente: Google Brasil Internet LTDA. Recorrido: Maria da Graça Xuxa Meneghel. Relatora: Ministra Nancy Andrighi. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/22026857/recurso-especial-resp-1316921-rj-2011-0307909-6-stj/inteiro-teor-22026859. Acesso em 06 set. 2020.

BRASIL. Superior Tribunal de Justiça (3ª turma). **Recurso Especial 1.660.168-RJ (2014/0291777-1)**. Recorrente: Yahoo! Do Brasil Internet LTDA. e Google Brasil Internet LTDA. Recorrido: Denise Pieri Nunes. Relatora: Ministra Nancy Andrighi. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/595923405/recurso-especial-resp-1660168-rj-2014-0291777-1/inteiro-teor-595923409. Acesso em 06 set. 2020.

BRASIL. Superior Tribunal de Justiça (4ª turma). **Recurso Especial 1.334.097-RJ (2012/0144910-7)**. Recorrente: Globo Comunicação e Participações S/A. Recorrido: Jurandir Gomes de França. Relator: Ministro Luís Felipe Salomão. Brasília, 15 de agosto de 2013. Disponível em: https://www.jusbrasil.com.br/diarios/58894344/stj-10-09-2013-pg-2572. Acesso em 06 set. 2020.

BRASIL. Superior Tribunal de Justiça (4ª turma). **Recurso Especial 1.335.153-RJ (2011/0057428-0)**. Recorrente: Nelson Curi e Outros. Recorrido: Globo Comunicação e Participações S/A. Relator: Ministro Luís Felipe Salomão. Disponível

em: https://www.conjur.com.br/dl/direito-esquecimento-acordao-stj-aida.pdf. Acesso em 06 set. 2020.

CANOTILHO, José Gomes.; MACHADO, Jónatas E. M.; GAIO JÚNIOR, Antônio Pereira. **Biografias Não Autorizadas *versus* Liberdade de Expressão**. Curitiba: Editora Juruá, 2014.

CASTELLS, Manuel. **A Sociedade em Rede**: Volume I. 8ª ed. Tradução: Roneide Venancio Majer com a colaboração de Klauss Brandini Gerhardt. São Paulo: Paz e Terra, 1999.

CASTRO, Catarina Sarmento e. **Direito da Informática, Privacidade e Dados Pessoais**. Coimbra: Almedina, 2005

CORRÊA, Gustavo Testa. **Aspectos jurídicos da internet**. 5 ed. São Paulo: Saraiva, 2010.

DE FLEUR, Melvin L., BALL-ROKEACH, Sandra. **Teorias da comunicação de massa**. Tradução: Octavio Alves Velho. Rio de Janeiro: Zahar, 1993.

DUCHEIN, Michel. **Les obstacles à l'accès, à l'utilisation et au transfert de l'information contenue dans les archives:** une étude RAMP. Paris: Unesco, 1983. Disponível em: http://unesdoc.unesco.org/images/0005/000576/057672fo.pdf. Acesso em: 06 set. 2020.

ENRIQUEZ, Eugène, "L'idéal type de l'individu hypermoderne: l'individu pervers?", *In*: AUBERT, Nicole (org.), **L'Individu hypermoderne**. Toulouse: Érès, 2004.

ESTADOS UNIDOS DA AMÉRICA. United States Supreme Court. **Griswold v. Connecticut**. v. 381 U.S. 479, 1965. Disponível em: https://supreme.justia.com/cases/federal/us/381/479/ , Acesso em: 06 set. 2020.

FERNÁNDEZ, Gabriela Rodríguez. Lo cotidiano del control en la gubernamentabilidad liberal del siglo XXI: una lectura desde Foucault, treinta años después. *In*: BESSA, C. Fernández; GORSKI, H. Silveira; FERNÁNDEZ, G. Rodríguez; BEIRAS, I. Rivera (ed.). **Contornos bélicos del Estado securitario**. Control de la vida y procesos de exclusión social. Barcelona: Anthropos, 2010.

FERRIGOLO, Noemi Mendes Siqueira. **Liberdade de expressão**: direito na sociedade da informação: mídia, globalização e regulação. São Paulo: Pillares, 2005.

FOUCAULT, Michel. **Vigiar e punir**: Nascimento da prisão. 20ª ed. Tradução: Raquel Ramalhete. Petrópolis: Vozes, 1999.

GUERRA, Sidney. **O direito à privacidade na internet**: uma discussão da esfera privada no mundo globalizado. Rio de Janeiro: América Jurídica, 2004.

HIGA, Paulo. Dados de 2,4 milhões de usuários de câmeras de segurança estavam expostos. **Tecnoblog**. 30 dez. 2019. Disponível em: https://tecnoblog.net/319514/wyze-vazamento-dados-usuarios-cameras-de-seguranca/ . Acesso em 06 set. 2020.

JENKINS, Henry. **Cultura de Convergência**. Tradução: Alexandria Susana. São Paulo: Aleph, 2008.

LEONARDI, Marcel. **Tutela e Privacidade na Internet**. São Paulo: Editora Saraiva, 2011.

LIMBERG, Têmis. **O direito à intimidade na era da informática**: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 10ª ed. rev. e atual. São Paulo: Saraiva, 2015.

MINIWATTS MARKETING GROUP. **World Internet Usage Statistics News and World Population Stats**. Disponível em: www.internetworldstats.com. Acesso em 06 set. 2020.

MONTEIRO, Renato Leite. Da proteção aos registros, aos dados pessoais e às comunicações privadas. *In*: MASSO, Fabiano del; ABRUSIO, Juliana; FLORENCIO FILHO, Marco Aurélio. (Org.) **Marco Civil da Internet** – Lei 12.965/2014. 1ª ed. São Paulo: RT, 2014, v.1, p. 139-153.

OLIVEIRA, Odete Maria de. **Teorias globais e suas revoluções**: elementos e estruturas. Ijuí: Ed. Unijuí, 2004.

OLSSON, Giovanni. **Poder político e sociedade internacional contemporânea**: governança global com e sem governo e seus desafios e possibilidades. Ijuí: Ed. Unijuí, 2007.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS – ONU. **Convenção das Nações Unidas contra a corrupção**. 31 de outubro de 2003. Disponível em: https://www.unodc.org/documents/lpobrazil/Topics_corruption/Publicacoes/2007_UNCAC_Port.pdf . Acesso em 06 set. 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS – ONU. **Declaração Universal dos Direitos Humanos de 1948**. 10 de dezembro de 1948. Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf . Acesso em 06 set. 2020.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS – OEA. Comissão interamericana de Direitos Humanos. **Declaração de princípios sobre liberdade de expressão**. Outubro de 2000. Disponível em: https://www.cidh.oas.org/basicos/portugues/s.Convencao.Libertade.de.Expressao.htm. Acesso em 06 set. 2020.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS – OEA. Pacto de San José da Costa Rica. **Convenção Americana sobre Direitos Humanos**. 22 nov. 1969. Disponível em: http://www.pge.sp.gov.br/centrodeestudos/bibliotecavirtual/instrumentos/sanjose.htm. Acesso em 06 set. 2020.

OST, François. **O Tempo do direito**. Tradução: Élcio Fernandes. Bauru: Edusc, 2005.

OXFORD UNIVERSITY PRESS. **Oxford English Dictionary**. 2nd ed. Oxford: Clarendon Press, 1989, v. 7.

PALLAZZI, Pablo A. **La transmissión internacional de datos personales y la protección de la privacidad**: Argentina, América Latina, Estados Unidos e la Unión Europea. Buenos Aires: Editora Ad-Hoc, 2002.

PIÑAR MAÑAS, Jose Luis. Introducción: Hacia un Nuevo Moledo Europeo de Protección de Datos. *In*: GAYO, Miguel Recio; CARO, Maria Álvarez (coord.). **Reglamento General de Protección de Datos – Hacia un nuevo modelo de privacidade**. Madrid: Editora Reus. 2016. p. 15-22.

RODOTÁ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RUARO, Regina Linden; SOUZA, Fernando Inglez de. **Cenários de regulação da proteção de dados pessoais e os desafios de uma tutela efetiva no ordenamento jurídico brasileiro**: a internet e suas implicações na privacidade e na proteção de dados pessoais. Interesse Público – IP, Belo Horizonte, ano 19, n. 103, p. 210, maio/jun. 2017.

SILVA, Felipe Stribe da. Proteção da intimidade nas redes sociais da internet: uma revisão do conceito de intimidade como forma de adaptação de seu sistema de proteção para os indivíduos membros das redes sociais da internet. **Revista Direitos Emergentes na Sociedade Global**, v. 2, n. 1, p. 109-141, jan./jun. 2013. DOI: https://doi.org/10.5902/231630547221. Disponível em: https://periodicos.ufsm.br/REDESG/article/view/7221#.X1onW3lKjIU. Acesso em 06 set. 2020.

SOUZA, Sérgio Ricardo de. **Controle judicial dos limites constitucionais à liberdade de imprensa**. Rio de Janeiro: Lumen Juris, 2008.

UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia, de 7 de dezembro de 2000. **Jornal Oficial das Comunidades Europeias**, Portugal, nº C 364, pp. 1-22, 18 dez. 2000.

UNIÃO EUROPEIA. Directiva 2002/58/CE do Parlamento Europeu e do Conselho da Europa, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas). **Jornal Oficial das Comunidades Europeias**, Portugal, nº L 201, pp. 37-47, 31 jul. 2002.

UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no

que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial das Comunidades Europeias**, Portugal, nº L 281, pp. 31-50, 23 nov. 1995.

VENTURA, Felipe. Governo de SP confirma que expôs dados pessoais de 28 mil habitantes. **Tecnoblog**. 25. out. 2019. Disponível em: https://tecnoblog.net/312170/governo-sp-confirma-expos-dados-pessoais-28-mil-pessoas/ . Acesso em 06 set. 2020.

VIEIRA, Tatiana Malta. **O Direito à privacidade na Sociedade da Informação**: Efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. Dissertação (Mestrado em Direito, Estado e Sociedade) – Faculdade de Direito, Universidade de Brasília, Brasília, 2007.

WHIPPS, Heather. How Gutenberg Changed the World. **Live Science**, 26 mai. 2008. Disponível em: https://www.livescience.com/2569-gutenberg-changed-world.html. Acesso em 06 set. 2020.

YAEL ONN, et al., Privacy in the Digital Environment. **Haifa Center of Law & Technology**, p. 1-12, 2005.